SurfControl®

Version 5.5

SurfControl Web Filter

Starter Guide

NOTICES

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published January 2008

Trademarks

Notices

TABLE OF CONTENTS

Chapter 1

Introduction

MICROSOFT ISA SERVER EDITION

SurfControl Web Filter for ISA integrates fully with Microsoft ISA server, in order to prevent web based threats. This edition of Web Filter also includes an anti-virus agent, which prevents infectious content by filtering viruses at the Web gateway.

HOW WEB FILTER AND ISA SERVER INTERACT

1 A client makes a request via the ISA Server for the resource.

2 The ISA Server challenges for authentication.

3 The client negotiates authentication parameters and requests the resource again.

4 The ISA Server connects to the target server and requests the resource.

5 Data starts coming down from the target servers.

6 If the policy is set to block this request, Web Filter resets this connection mid-transmission.

7 If the request was blocked, the denied page is returned to the user.

Depending on whether you are using ISA Server 2000, 2004 or 2006, SurfControl Web Filter has the following features:

ISA SERVER 2000

Table 1-1 Features of SurfControl Web Filter for Microsoft ISA Server 2000

Feature	Description
Quick and easy to configure	The Web Filter Configuration Wizard guides you through the configuration process, so that you can begin filtering Web content as soon as possible.
Seamlessly integrates with ISA as an ISAPI filter	You can install Web Filter directly on to an existing ISA Server, for an easy and secure filtering solution.
Ideal for implementing Acceptable Use Policies	It's easy to set up and maintain powerful, flexible rules that enforce your Acceptable Use Policy.
Transparent to the desktop user	Users in your organization know immediately if they have browsed to a page that breaches your Acceptable Use Policy.

ISA SERVER 2004 AND 2006

In addition to the above features, SurfControl Web Filter for ISA Server 2004 and 2006 offers the addition of an application filter as part of the Firewall Service. This allows the management and reporting of protocols beyond HTTP, HTTPS and FTP when using the ISA Server firewall.

SYSTEM REQUIREMENTS

The minimum and recommended specifications for installing SurfControl Web Filter and SurfControl Report Central are described in the sections below.

HARDWARE REQUIREMENTS

The tables below outline the specific hardware requirements, which are dependent on whether the Anti-Virus Agent is enabled or not.

Table 1-2 Hardware Requirements - Anti-Virus Agent disabled

Component	Minimum	Recommended
Processor	Intel Pentium IV	Xeon
Memory	1GB RAM	2 GB RAM
Network	Ethernet card	
ISA Servers required in an array	• 1 server - supports 0-15,000 users • 2 servers - supports 15,000-17,500 users • 3 servers - supports 17,500-22,500 users **Note:** These requirements will vary dependent upon actual Web traffic characteristics.	

Table 1-3 Hardware Requirements - Anti-Virus Agent enabled

Component	Minimum
Processor	2 x Pentium Dual Core Xeon
Memory	1 GB RAM
Network	Ethernet card
ISA Servers required in an array	• 1 server - supports 0-2,000 users • 2 servers - supports 2,000-7,500 users • 3 servers - supports 7,500-10,000 users **Note:** These requirements will vary dependent upon actual Web traffic characteristics.

GENERAL SYSTEM REQUIREMENTS

The recommended general specifications for your Web Filter installation are shown in the table below:

Table 1-4 Web Filter System Requirements

Component	Minimum	Recommended
Supported Operating Systems (with latest Service Packs)	• Windows 2000 Server • Windows 2000 Advanced Server • Windows Server 2003 (Standard or Enterprise Edition)	
Supported database platforms (with latest Service Packs)	• Microsoft SQL Server Express (Requires Windows Installer 3.1 if installing on a Windows 2000 computer) • Microsoft SQL Server 2000 • Microsoft SQL Server 2005 **Note:** SurfControl recommends that you install SQL Server Express or SQL Server before you begin installing Web Filter.	
Disk Space	1 GB free	5 GB free
Optional NetWare user name support	If you plan to monitor users based on NetWare user names, then you must install the Novell NetWare Client (version 5.x) over IP on the Web Filter server prior to installing Web Filter.	
Optional Windows user name support	If you plan to monitor users based on Windows user names, then you must be using MS NT4 or Active Directory domain controllers.	
Microsoft ISA Server	• ISA Server 2000 (Standard or Enterprise Edition) with SP2 • ISA Server 2004 (Standard or Enterprise Edition) with SP2 or later • ISA Server 2006 (Standard or Enterprise Edition)	
Web browser	Microsoft Internet Explorer 5.0	Microsoft Internet Explorer 7.0
Applications	Adobe Acrobat Reader 6 or higher for viewing reports and documentation in pdf format.	

SQL SERVER LICENSING

If you have purchased SQL Server under a Server plus Device CALs, or a Server plus User CALs license model, you will need additional client access licenses (CALs) for the following:

- A single Web Filter remote administration client installed.
- SRC installed on a different server to Web Filter.

Note: For each additional remote administration client, an additional CAL is required.

For more information about SQL Server CAL requirements, go to the following Microsoft pages:

- http://www.microsoft.com/sql/howtobuy/default.mspx
- http://www.microsoft.com/resources/sam/lic_cal.mspx#perprocessor

Chapter 2

Installation Decisions

INTRODUCTION

There are certain decisions you must make before you start to install SurfControl Web Filter, based on the design of your network.

During the Configuration Wizard part of the installation, specific information is required which relates to your network topology, database location and how network user names should be resolved. Therefore it is important to consider how you will deploy Web Filter, to enable the most effective monitoring and filtering solution for your environment. The following sections describe the different areas that should be considered before you start. See "Further Configuration" on page 51 for more details.

Network Considerations (page 9)

- How do you install Web Filter on to your ISA Server Network?

User Name Resolution (page 12)

- How do you want Web Filter to handle user name resolution?
- How do you want to monitor users (IP address, workstation name, EUM, NetWareEUM, EUM Login Agent)?

Database Options (page 21)

- What database platform do you plan to use (SQL Server Express or SQL Server)?
- How do you want Web Filter to connect to the database (Windows authentication or SQL authentication)?

Other Considerations (page 24)

- Content information
- Which e-mail notifications should Web Filter send?
- Do you need to install the Remote Administration Client?

NETWORK CONSIDERATIONS

You can install SurfControl on a single ISA Server or in multi-server arrays. In an ISA Standard Edition installation, Web Filter is installed on a single ISA Server. In an ISA Enterprise Edition environment, Web Filter is installed on multiple servers.

DEPLOYMENT RECOMMENDATIONS

SurfControl recommends the following when deploying Web Filter for ISA Server:

- If Web Filter for ISA Server is used as a proxy, it does not need to be installed in a specific location in the LAN. However, if it is used as a firewall, consult the Microsoft ISA templates for network placement recommendations.
- Use a firewall to deny HTTP traffic from all IP addresses except for the ISA server.
- Firewall clients should be configured so that the browser uses a proxy service.

DMZ RECOMMENDATIONS

In a perimeter network (DMZ) installation, Web Filter is installed on one or more ISA Servers located between a perimeter firewall and an internal firewall. SurfControl recommends the following when deploying Web Filter for ISA Server in the DMZ:

- If the ISA Server is part of the DMZ domain, Web Filter for ISA Server should be a member of the domain that users log into.
- Is there a one-way or two-way trust relationship between the Web Filter ISA Server and the corporate domains? Two-way trust relationships are very reliable. One-way trusts will cause problems if configured to trust the wrong way.
- Are there multiple domain controllers? The ports required to query the domain controllers should already be open via System Policy LDAP to localhost. If not, check to see which ports if any, must be opened for this purpose.

When Web Filter for ISA is deployed in a DMZ, it may be unable to query the domain controllers for a variety of reasons:

- It cannot resolve the IP addresses of the domain controllers.
- It is unable to authenticate to the domain controllers.
- Access is blocked by a firewall, preventing Web Filter from enumerating groups using NT objects.

To Resolve a domain controller name resolution issue:

- Add an entry to the LMHosts file on the Web Filter server(s) for the domain controllers. See the following Microsoft KB article for more information: http://support.microsoft.com/Default.aspx?kbid=180094
- Enable NETBIOS over IP on the Web Filter server(s).

To resolve an authentication issue:

- Use a Local Admin account to log into the Web Filter server(s). This account should also be a member of the domain administrators group in the DMZ, and an account with the same name and password should exist in the corporate domain. Use this logon account for the Web Filter services also.

To resolve a firewall access issue:

- Set up a child domain with a trust relationship between the domain controllers with Web Filter for ISA a member of the child domain.
- Open up ports on the internal firewall where necessary.

FIREWALL PORT CONFIGURATION

Web Filter for ISA requires you to edit your system policy to allow Web Filter to communicate across certain network ports. Opening up these ports at the firewall will enable you to use all of the available Web Filter services. For instructions on setting up ISA policy rules for Web Filter services, go to the section on "Firewall Policy Rules" on page 65. The table below describes which ports need to be configured at the firewall for each Web Filter service you want to use:

Table 2-1 Web Filter communication ports

Web Filter Service	Port
Corporate Network Detection Service	51118
SMTP E-mail Notifications	25
EUM Login Agent	61695
EUM Login Agent for Netware	61696
Group enumeration in Active Directory (LDAPS)	636
Group enumeration in Active Directory and Netware (LDAP)	389
Live Updates	Allow outbound access to *.surfcontrol.com
Real-Time Monitor	5000
Remote Administration Client (UDP)	1024 - 65535
SurfControl Report Central	Allow inbound access to 8888 and/or 8443
SQL Server (Remote installations only)	Allow inbound and outbound access to 1433 -1434
User Name Resolution (NetBIOS)	139
Workstation name resolution	53
Workstation name resolution (WINS)	42

ISA SERVER AUTHENTICATION

You can use ISA Server to authenticate your users, if you don't want to use NetBIOS or EUM. This procedure is different, depending on whether you are using ISA Server 2000 or 2004 and above.

ISA Server 2000

To configure ISA Server 2000 for User Authentication, perform the steps outlined in the following instructions:

1 Open the **ISA Management Console** from the **Start > Programs** menu.

Find your machine name within the ISA tree. This will be listed within **Internet Security and Acceleration Server\Servers and Arrays**.

2 Right-click on your machine name and choose **Properties** from the pop-up menu.

3 Select the **Outgoing Web Requests** tab.

4 Select the **Ask unauthenticated users for identification** check-box.

5 In the same dialog double-click your machine name in the Server column of the identification pane. This can be found in the Identification Section. The **Add/Edit Listeners** dialog is displayed.

6 Select the **Integrated authentication** check box.

7 Select the **Basic with this domain** check-box and click **Yes** on the **ISA Server Configuration** pop-up.

8 Click the **Select Domain** dialog. Alternatively, use the **Browse** button to navigate to your domain.

9 Click **OK** and close all of the open dialogs until you return to the Properties dialog for your ISA Server.

10 Click **OK** on this dialog and select the **Save Changes and restart the service(s)** radio button on the **ISA Server Warning** pop-up. Click **OK** again.

ISA Server 2004/2006

To configure ISA Server 2004 or 2006 for User Authentication, perform the steps outlined in the following instructions:

1 Open the **ISA Management Console** from the **Start > Programs > Microsoft ISA Server** menu.

Find your machine name within the ISA tree. This will be listed within **Internet Security and Acceleration Server 2004**.

2 Expand the **Configuration** option.

3 Select **Networks**.

4 Select the network you want to monitor and select **Edit Selected Network** from the **Tasks** pane.

5 From the **Network Properties** dialog box, select the **Web Proxy** tab.

6 Click **Authentication**.

7 From the **Authentication** dialog box, select **Require all users to authenticate**.

8 Click **OK** to close the Authentication dialog box.

9 Click **OK** to close the network **Properties** dialog box.

USER NAME RESOLUTION

By default, SurfControl Web Filter doesn't monitor user names. The **Configuration Wizard** enables you to monitor your users by name, in the following ways:

- By using ISA Server to authenticate user names. This also prevents having to install EUM on all your domain controllers. This is the recommended method.
- By installing the supplied **Enterprise User Monitor (EUM)** utility, which you can install either on your domain controllers, Novell NDS tree servers or via a logon program stored on your network.
- By issuing a NetBIOS query based on the MAC address.

Note: Web Filter supports three monitoring methods: user name, workstation name or IP address.

SurfControl recommends monitoring by user because:

- Monitoring by workstation name only identifies the machine requesting the data, not the user who originated the request.
- Monitoring by user name is more convenient in a workplace where employees share or swap machines frequently.
- Monitoring by user name enables you to filter users based on NT Users and Groups.
- Monitoring by user name makes it easier to track users that frequently login to multiple machines.

Web Filter places data on the Monitor with the following precedence:

1 User name resolved with NetWareEUM.

2 User name resolved with EUM.

3 User name based on NetBIOS query.

4 Workstation ID.

5 IP address.

EUM

EUM accesses Windows NT, Windows 2000 and 2003 security auditing data to resolve user names. This provides Web Filter with the ability to monitor traffic on a routed network by user name. EUM provides Web Filter with continuous, accurate reporting of logon activity by user name.

For example, when jsmith attempts to access http://www.cnn.com, Web Filter sees jsmith's IP address in the HTTP request. EUM provides the missing link by receiving data from the domain controllers regarding jsmith's identity.

METHODS OF INSTALLING EUM

You can install EUM in one of two ways:

1 Install an EUM Agent on your domain controllers or Novell NetWare NDS Tree Server.

2 Install an EUM Login Agent on your network that can monitor all users via a login script. (page 17)

Installing the EUM Agent on your Domain controllers works well in a LAN environment where all users log on to the Windows domain. If you do not have access to, or do not wish to install the EUM Agent on your domain controller, you can use the EUM Login Agent.

THE EUM AGENT ON DOMAIN CONTROLLERS

You can install the EUM Agent on domain controllers which have the following operating systems:

- Windows NT
- Windows 2000
- Windows 2003 (Standard and Enterprise)
- Windows 2003 x64 (Standard and Enterprise)

There is also a version of the EUM Agent that works with Novell NetWare. This is explained further in "NetWareEUM" on page 16.

During the installation, the configuration file **scua.ini** is installed into the **c:\Surfcontrol User Agent** folder on each domain controller. This file contains connection information about your Web Filter server(s) and identifies ignored users, which are specified during the installation. Additional domain controllers and/or ignored users can also be added to your EUM Agent configuration at a later date. For further details about installing the EUM Agent and post configuration tasks, refer to the following sections:

- "Installing the EUM Agent on your domain controllers" on page 53
- "Making changes to the EUM Agent configuration" on page 55

EUM on Windows 2000 and 2003 domain controllers

The EUM agent is installed on to Windows 2000 and 2003 domain controllers as a driver file called **ScSubAuth.dll**. If you are installing EUM on a Windows 2003 x64 operating system, the driver file **ScSubAuth_AMD64.dll** is loaded on to the domain controller during installation. When EUM is installed on to a Windows 2000 or 2003 server, Web Filter uses Microsoft's Sub-Authentication to resolve user names.

EUM on Windows NT domain controllers

Web Filter installs the EUM User Agent (UA) on to Windows NT domain controllers as a service (SurfControl User Agent service; ScUserAgent.exe). During EUM installation, Web Filter configures NT domain controllers to record Successful Logons to the security log (event 528). If you make changes to this audit policy and disable event 528 logs (Successful Logon), EUM will not work correctly.

Confirm that event 528 logs are enabled by performing the following:

1 From the Web Filter server, select **User Manager for Domains** from the **Programs > Administrative Tools** menu.

2 From the menu, select **Policies Audit**. Ensure that **Audit these Events** is checked.

3 Ensure security logs are set to overwrite as needed. Do not manually clear the security logs.

Before installation

Prior to installing the EUM UA on to an NT domain controller, ensure the trust relationships are set up for multiple domain environments.

Note: The trust relationship should be configured so that Web Filter is Trusted, and all other domains are Trusting.

During installation, Web Filter installs the EUM UA on to each domain controller. Before installing EUM, ensure the following:

- The Web Filter server must have a static IP address.
- The installer must be logged into the Web Filter server as a user with domain administration rights.
- For a successful automatic installation, Web Filter must be able to see the domains that require EUM. Make sure Web Filter is located in the appropriate domain.
  - In a two-way trusted environment, the Web Filter server can be located in any domain.
  - If a one-way model is in use, the Web Filter server should be located in the master domain (this enables Web Filter to see all other domains).
- For Windows NT domain controllers, make sure the security logs of all domain controllers are set to overwrite events as needed.
- By default, EUM uses port 61695 to communicate with the Web Filter server. Perform the following steps to change the port:
  1) Add the following key to the SurfControl registry:

     `HKEY_LOCAL_MACHINE\SOFTWARE\JSB\SurfControlScout\UserAgentPort`

  2) Add the key as a DWORD, specify a decimal value (default is 61695).
  3) Stop and start the Web Filter service.
  4) Update the scua.ini file on the domain controllers to reflect the port changes.
- SurfControl recommends installing EUM when there are few or no users on the network or when a forced log off can be scheduled.
- During installation, you'll be prompted to identify specific user accounts that UA should ignore. You should only use this option for accounts similar to SMS or service accounts (for instance, backup.exe, anti-virus updates, servers).

Caution: Ignoring valid user accounts will result in mis-identification.

NETWAREEUM

Web Filter also enables you to monitor users by their Novell NetWare user name. The Novell version of EUM is called NetWareEUM. NetWareEUM works in the same way as EUM. Web Filter installs a User Agent on to each Novell NDS tree server.

Caution: Web Filter does not support Novell 4.x. If you need to resolve Novell 4.x users, authenticate all users on an NT or 2000 domain controller and use EUM to resolve the user names.

Before installing NetWareEUM, ensure the following:

- Install NetWare's Client 32 (as Preferred TCP/IP Protocol) on to the server. SurfControl recommends you do this before installing Web Filter.
- Network must be using Novell 5 or 6 over IP.
- The Web Filter server must have a static IP address. You need to manually edit the scua.ini file to add the host name or IP address and port number of any Web Filter servers. See "Add Web Filter Servers to NetWare EUM" on page 58 for more details.
- By default, NetWareEUM uses port 61696 to communicate with the Web Filter server. Perform the following steps to change the port:
  1) Add the following key to the registry:

     `HKEY_LOCAL_MACHINE\SOFTWARE\JSB\SurfControlScout\NWUserAgentPort`

  2) Add the key as a DWORD, specify a decimal value (default is 61696).
  3) Stop and start the Web Filter service.
- SurfControl recommends installing NetWareEUM when there are few or no users on the network or when a forced log off can be scheduled.

Ignoring Users in NetWare EUM

Users such as administrative groups, other NetWare servers or users using ZENworks need to be ignored by the NetWare server where Web Filter is installed. This requires the `scua.ini` file to be edited.

Ignoring other NetWare servers can prevent caching problems, especially when setting the Logging level to 2. See below for more details.

Logging Levels

A log file `surflog.txt` will be created and stored in the same directory as the `scua.ini` and `nweum.nlm` files. This holds details of various events. In a default installation this is located in:

`C:\Program Files\SurfControl\Web Filter\NetWare`

In the scua.ini file you can set the logging level for events to be stored in this file. The levels are as in the table below. The default logging level is 1:

Table 2-2 Logging Levels

Value	Logging detail
0	No logging.
1	Important events - Startup, Shutdown, Errors, Connection with Web Filter installations, Connection failures, Disconnections.
2	Login events such as Ignored Users.
3	Combination of levels 1 and 2.

THE EUM LOGIN AGENT

The Login Agent enables you to use the EUM without having to install anything on your domain controllers. It works by saving a supplied program (`ScEumLoginAgent.exe`) and a configuration file (`EumLogin.ini`) to a location on your network that is accessible to all users. You must then perform the following to enable the login agent to work.

Installing the Login Agent on NT Domains

1 Manually configure the `EumLogin.ini` file.

2 Create a new log on script, or modify an existing one to call the `ScEumLoginAgent.exe`.

3 Use the `/INTLOGOFF` parameter to allow log on and log offs to be handled by the same script. See "Configuring a logon and logoff script" on page 20 for more details.

Installing the Login Agent on Windows 2000 and 2003

1 Manually configure the EumLogin.ini file.

2 Create a new log on and log off script, or modify an existing one, to call the `ScEumLoginAgent.exe`. See "Configuring a logon and logoff script" on page 20 for more details.

3 Add traffic from the ScEumLoginAgent program as an exception to the Windows Firewall that allows the ScEumLoginAgent program to operate. See "Add an Exception to the Windows Firewall" on page 20 for more details.

Login Agent Location

The Login Agent program and .ini file can be found in the following location in a default install:

`C:\Program Files\SurfControl\Web Filter\EnterpriseUserMonitoring\LoginAgent`

Note: The ScEumLoginAgent is not supported on client machines running Microsoft Windows NT4.

The EumLogin.ini file

Below is a copy of the supplied .ini file

```
[Surfcontrol_Servers]

# The [Surfcontrol_Servers] section of the EumLogin.ini file is used to set the

# server names to be used for each instance  of SurfControl Web Filter.

#Servers=SERVERNAME,127.0.0.1


[SERVERNAME]

# Section name section, which specifies the SurfControl Web Filter server and its

# listening port number. The ServerName can be an IP Address or Computer Name

# value e.g.

# Port=61695

# NetwarePort=61696


#[127.0.0.1]

#Port=61695

#NetwarePort=61696


[Continuous_Mode]

# This is the interval by which the Login EXE will send login details to SWF servers

# when in continuous mode. Value is in seconds e.g.

# Interval=900

Interval=900


[Retry_Connection]

# Number of times we will attempt to connect to SWF service e.g.

# Retry=5

Retry=5
```

How to configure the file

The table below describes the various sections of the EumLogin.ini file and how to enter your information.

Table 2-3 The EumLogin.ini file sections

Section	What to enter
`[Surfcontrol_Servers]`	Enter the name, or IP address, of each server in your organization that Web Filter is installed upon. The format is: `Servers=Servername1,Servername2,127.0.0.1` **Note:** Do not leave spaces between the server names.

`[SERVERNAME]`	For each server specified in `[Surfcontrol_Servers]`, make an entry along with the default Web Filter listening port (61695) for Windows, or the default port (61696) for Netware.
	For example, the format for a Windows 2000 or 2003 domain is:
	`[Servername1]`
	`Port=61695`
	`[Servername2]`
	`Port=61695`
	`[127.0.0.1]`
	`Port=61695`
	The format for a Netware domain is:
	`[Servername1]`
	`NetwarePort=61696`
	`[Servername2]`
	`NetwarePort=61696`
	`[127.0.0.1]`
	`NetwarePort=61696`

`[Continuous_Mode]`	The Login Agent runs in continuous mode. The agent will send log on and log off details to the servers specified in `[Surfcontrol_Servers]` at a specified interval (in seconds). The default setting is 900 seconds. The format is: `Interval=900`
`[Retry_Connection]`	If a connection to any of the servers specified in `[Surfcontrol_Servers]` is dropped, the Login Agent will try to re-connect. This entry specifies how many times the agent will attempt to re-connect. If connection is not re-established after the number of times specified, the agent will wait for the interval specified in `[Continuous_Mode]` before attempting to connect again. The maximum value is 5. If you enter a value higher than 5 the Login Agent will only try 5 times. The format is: `Retry=5`

Configuring a logon and logoff script

You need to create a new logon and logoff script, or modify an existing one, to call the EUM Login agent (`ScEumLoginAgent.exe`). The EUM Login Agent file should be placed in an area on the network which is accessible to all users. The following parameters can be used in the logon script:

Note: A logoff script is not required for NT domains.

- `/LOGOUT` - This is used if the agent is called by a log off script. If this parameter is not used, the agent will assume it is a logon script.
- `/NETWARE` - This command line parameter is used in a Netware environment. Use this in the login script to return the Netware user name to the EUM Login Agent. This will ensure that the default Netware port (61696) is loaded from the EumLogin.ini file. If this parameter is not specified, the Windows username will be returned by default to the EUM Logon Agent.
- `/NOCONT` - This is used to run the agent in non-continuous mode. The agent will send the user name details once to the server(s) and then terminate. If this parameter is not used, the agent will run in continuous mode.
- `/TRACEMODE` - Use this command line parameter if you are experiencing problems with the agent. Trace messages will be stored in a log file called `EumLoginTrace.log`. This file will be stored in the logged on user's temporary folder. The location of this folder is determined by the following:
  - The path specified by the TMP environment variable.
  - The path specified by the TEMP environment variable.
  - The path specified by the %USERPROFILE% environment variable.
  - The Windows directory.

Add an Exception to the Windows Firewall

The Windows Firewall will prevent the ScEumLoginAgent application from sending traffic to the network. To allow the EUM Login Agent to function requires an Active Directory group policy to be created or updated to add the traffic from the application as an exception to the firewall. For more details on these options consult our Knowledge Base article 1775.

The Knowledge Base can be found at: http://kb.surfcontrol.com

DATABASE CONSIDERATIONS

Before you start to install Web Filter, you should decide:

- Which database platform you plan to use (SQL Server Express or SQL Server).
- How Web Filter will connect to the database (Windows or SQL authentication).

DATABASE PLATFORMS

Web Filter uses SQL Server Express, or a fully-licensed version of SQL Server 2000 or 2005. SurfControl recommends that you ensure your choice of database platform is installed and running, before attempting to install Web Filter. SurfControl recommends that you use SQL Server rather than SQL Server Express for the following reasons:

- SQL Server allows greater scalability.
- SQL Server enables you to fine-tune database performance.
- SQL Server is more suitable for environments with heavy Web traffic.
- SQL Server Express has a maximum size of **4GB**.

Web Filter connects to the database using a fully-qualified connection string. This string contains all the details required to connect to a database including database type, name of the server, user ID, password, and database name. Using a connection string does not require the creation of Data Source Names (DSN), therefore, any Web Filter client or server on the network can access the database without creating a link through the ODBC driver.

SQL Server Express

If you are not using a SQL Server database, you need to install SQL Server Express. SurfControl recommends you install your database platform before installing Web Filter. If you want to use SQL Server Express, be aware of the following:

- You must install **.NET Framework 2.0** before installing SQL Server Express.
- If installing on a **Windows 2000** computer, you must install **Windows Installer 3.1** before installing SQL Server Express.
- You must install SQL Server Express as a **Default Instance** when prompted during installation.
- You must install the **Database and Connectivity Components** when prompted during installation.
- You must perform the steps outlined below after installing SQL Server Express, and before installing Web Filter.
- By default, SQL Server Express runs as a Network Service. When performing a database archive or restore, it needs to run with a local admin account to be able to access drive C.

The following post SQL Server Express installation configuration is taken from the MSDN Blog entry: http://blogs.msdn.com/sqlexpress/archive/2004/07/23/192044.aspx which explains the steps in more detail. The Post SQL Server Express Installation Configuration steps are as follows:

1 Make sure SQL Server Express is running correctly (assumes a default install).

2 Open a Command Prompt.

3 Type the following: `sqlcmd -S.\sqlexpress`

4 You should get a prompt like this: `1>`

5 Type: `Exit to exit sqlcmd`

6 Open the **SQL Computer Manager**.

7 Expand **Server Network Configuration**.

8 Expand Protocols for **SQLEXPRESS**.

9 Enable **Np** (for local and remote access).

10 Enable **TCP** (for local and remote access).

11 Restart SQL Server Express.

To access SQL Server Express database tables, you can use the Windows OSQL utility from the command prompt. For more details about the OSQL utility, visit www.microsoft.com.

For more information about SQL Server Express, visit: http://www.microsoft.com/sql/editions/express/default.mspx

SQL Server

If you have SQL Server on your network, you should plan to create the database on that server (you can create and configure the database during the installation process). SurfControl recommends installing SQL Server on a dedicated server. If you plan to use a SQL Server database, but have not installed Microsoft SQL Server, complete the following tasks before installing Web Filter:

1 Install SQL Server on the designated server; this can be the same machine as the Web Filter server.

2 Make sure your server has the minimum resources listed in the table below.

Table 2-4 SQL Server minimum requirements on Web Filter server

# Users	Server Specification
<500	Intel Pentium IV, 2 GB RAM, 1.2 GHz processor, 10 GB hard drive.
500 - 1000	Intel Pentium IV, 3 GB RAM, 1.4 GHz processor, 20 GB hard drive.
1000 - 5000	Intel Pentium IV, 5 GB RAM, 1.4 GHz processor, 40 GB hard drive.
>5000	Intel Pentium IV, 7 GB RAM, 1.8 GHz processor, 60 GB hard drive.

3 Configure SQL Server to limit memory and processors when running both Web Filter and SQL Server on the same computer.

- There should only be one database owner (db_owner) per database.
- If you need to have multiple user accounts with database access, the other users should only have db_datareader and db_datawriter permissions.

Caution: Install SQL Server with the default setting of case insensitivity, including case insensitivity for Dictionary Order. Choosing case sensitivity may cause problems when installing Web Filter.

Reasons to Install SQL Server on a Dedicated Server

Use SQL Server 2000 or 2005 on a dedicated server if your organization:

- Needs to store large amounts of data (for instance, you have a large number of users, high Internet activity, or need to retain data for an extended period).
- Requires more than one Web Filter server (collector) to consolidate data in a single database.
- Plans to store Web Filter and SurfControl E-mail Filter data on the same SQL Server installation.

Make sure your dedicated SQL Server has the minimum resources listed in the table below:

Table 2-5 SQL Server minimum requirements for large environments

# Users	Computer Specification
<500	Intel Pentium IV, 1 GB RAM, 1.2 GHz processor, 10 GB hard drive
500 - 1000	Intel Pentium IV, 2 GB RAM, 1.4 GHz processor, 20 GB hard drive
1000 - 5000	Intel Pentium IV, 4 GB RAM, 1.4 GHz processor, 40 GB hard drive
>5000	Intel Pentium IV, 6 GB RAM, 1.8 GHz processor, 60 GB hard drive

DATABASE AUTHENTICATION

Web Filter supports both Windows authentication and SQL authentication. SurfControl recommends Windows authentication because it is easier to use and compliant with Microsoft's security recommendations. If you choose SQL authentication, any configured connections must be re-established if the username or password of the SQL user account (e.g. SA) changes. With Windows authentication, you can change the username and password without having to reconfigure the database connection.

Windows Authentication

If you choose to use Windows authentication, make sure domain rights are correctly configured between the Web Filter server and the SQL Server database. The Web Filter installer account requires SQL Server database creator rights.

SQL Authentication

If you choose to use SQL authentication, you will need to create a SQL Server login specifically for Web Filter. This login is required for creating the database and will be used for all Web Filter database activities.If you choose to connect to the SQL database using SQL authentication, make sure the SQL Server is configured to support SQL Server and Windows NT authentication.

OTHER CONSIDERATIONS

This section contains general information that you should be aware of when installing and configuring SurfControl Web Filter.

INTERNET THREAT DATABASE

SurfControl's Internet Threat Database is the best category database in the Internet security industry and provides the most accurate, current, and relevant content listing available. The Internet Threat Database includes:

- 55 structured categories.
- 24 million sites, including more than 3.5 billion web pages.
- International content, including 70 languages and over 200 countries.
- Daily updates (more than 100,000 new sites a week).
  - The Internet Threat Database is stored in an encrypted, size-optimized file called `SurfControl Categories.csf`.
  - Incremental updates (up to 60 MB) are stored in an encrypted file called `SurfControl Categories.cdb`.
  - With Web Filter, you can manually categorize destinations; these are added to the `SurfControl Manual Categories.ucf` file.
  - VCA categorized destinations are added to the `SurfControl VCA Categories.ucf` file.

Web Filter checks the categorization files in the following order:

1 Manually-categorized sites (`SurfControl Manual Categories.ucf`).

2 Incremental updates (`SurfControl Categories.cdb`).

3 Internet Threat Database (`SurfControl Categories.csf`).

4 VCA categorized sites (`SurfControl VCA Categories.ucf`).

CATEGORIZATION OPTIONS

You can select whether to send feedback on uncategorized sites back to SurfControl, and how Web Filter categorizes your own domains.

Internet Threat Database Improvement Program

When Web Filter encounters an uncategorized Web site, it can send the details anonymously to SurfControl. This helps SurfControl to improve the effectiveness of the Internet Threat Database in future updates.

Company & Intranet

You can enter your company domains and Intranet site addresses during the Configuration Wizard so that Web Filter categorizes them as **Company & Intranet**.

You can change the **Customer Feedback** and **Company & Intranet** settings From the **Web Filter Settings** in the Enterprise Manager. See the *Administrator's Guide* for more details.

E-MAIL NOTIFICATIONS

Web Filter can automatically notify the system administrator when any of the following events occur:

- **Service running status change** - If the status of any of the Web Filter services changes (for instance, from Running to Stopped).
- **Internet Threat Database license reminders** - If the Internet Threat Database license is close to expiring.
- **Scheduled task failures** - If any scheduled tasks fail to run.
- **ISA 2004 event notifications** - If the connection is lost between the ISA Server 2004 or 2006 and the Web Filter service, a notification will be sent.

Note: The ISA 2004 event notifications are not available for ISA Server 2000.

If you decide to enable e-mail notifications, you will need to know the hostname or IP address of your mail server and will need to identify an administrator that will receive the notifications.

Caution: Entering E-mail server, Recipient and From e-mail address details from within Web Filter will overwrite any settings present in ISA Server for the **Server not responding** and **Intrusion detected** alerts.

REMOTE ADMINISTRATION CLIENT

You can administer Web Filter from a remote location by installing the Remote Administration Client. You can use the Remote Administration Client to:

- View monitored traffic.
- Create and edit rules.
- Run reports.
- Start and stop the Web Filter Service.
- Start and stop the Scheduler Service.
- Access the Real-Time Monitor.

Before installation, make sure the Remote Administration client computer meets the minimum requirements as listed in the table below:

Table 2-6 Remote Administration Client minimum requirements

Component	Minimum	Recommended
Processor	Intel Pentium III	Intel Pentium IV
Memory	256 MB RAM	512 MB RAM
Supported Operating Systems (with latest Service Packs)	Windows 2000 Professional or Server Windows 2000 Advanced Server Windows Server 2003 Standard and Enterprise Editions Windows XP Professional Windows Vista Business and Enterprise Editions	
Network	Ethernet card	
Disk Space	5 GB free	
Web browser	MS Internet Explorer 5.0	MS Internet Explorer 7.0

PRIVACY EDITION CONSIDERATIONS

In certain European countries, there are laws which forbid the browsing details of users to be seen by monitoring software, unless express permission is given by a manager and a union representative. The Privacy Edition of SurfControl Web Filter enables companies in those countries to comply with this legislation.

You can only upgrade from the previous Privacy edition (5.0) to version 5.5. You cannot upgrade from any standard version of Web Filter to the Privacy edition. For more details on the Privacy Edition features, see the *Administrator's Guide*.

Chapter 3

Installing Web Filter

INTRODUCTION

The following sections show you how to install Web Filter Service Pack 3 along with instructions on how to install SQL Server and Web Filter version 5.5, if you have not already installed these products. There are three steps to installing Web Filter Service Pack 3:

- **Install SQL Server** - You must install SQL Server before installing Web Filter V5.5. If you have not installed SQL Server already then go to See “Installing SQL Server Express (optional)” on page 29.
- **Install Web Filter V5.5** - Once you have installed SQL Server you need to install Web Filter V5.5. If you have installed SQL Server but not Web Filter V5.5 then go to See “Installing SurfControl Web Filter” on page 30.
- **Install Service Pack 3** - Once you have installed SQL Server and Web Filter V5.5 you are ready to install Service Pack 3. See See “Installing Service Pack 3” on page 48.

This chapter explains how to install SurfControl Web Filter. There are six stages to the installation process, which are explained in the table below:

Table 3-1 Installation Process

Database platform preparation	If you have chosen **SQL Server Express** as your database platform, download and install it from the Microsoft Web site. See "Installing SQL Server Express (optional)" on page 29.
Product preparation	If you plan to monitor **NetWare user names**, install the **NetWare client** on to the **Web Filter server**.
Product installation and Configuration Wizard	Install **Web Filter** (complete installation) on the **Web Filter server**.
Remote Administration	If you want to administrate the **Web Filter server** from a remote location, install the **Remote Administration** client on the remote computer. Install the VCA client if required.
Post installation	If you plan to monitor Windows users by user name, install EUM, either by: • Installing the **EUM Agent** on all your domain controllers or **NetwareEUM** on to your NDS servers. • Installing the **EUM Login Agent** on your network and editing the supplied configuration file.
Report Central	Download and install SurfControl Report Central from: http://www.surfcontrol.com.

INSTALLING SQL SERVER EXPRESS (OPTIONAL)

If you plan to use **SQL Server Express** for your database, you must install it in the following order before installing Web Filter:

1 Download and install **.NET Framework 2.0** from http://msdn.microsoft.com/netframework/

2 If installing on a **Windows 2000** computer, download and install **Windows Installer 3.1**.

3 Download and install SQL Server Express from http://www.microsoft.com/sql/editions/express/default.mspx.

Note: You must install the Database and Connectivity Components when prompted during installation.

4 Perfom Post SQL Server Express Installation Configuration as described in the section on SQL Server Express.

You need to run SQL Server Express with a local admin account to be able to perform database management tasks such as Archive and Restore, as these tasks require access to drive C on your server. You may be requested to restart the server after installing SQL Express.

INSTALLING SURFCONTROL WEB FILTER

You can cancel the installation of Web Filter at any time by clicking **Cancel**. You will have to restart the installation process if you decide to run the install again at a later date.

Caution: The Microsoft firewall service is temporarily stopped and restarted during the Web Filter installation process, and as a result will interrupt Web browsing.

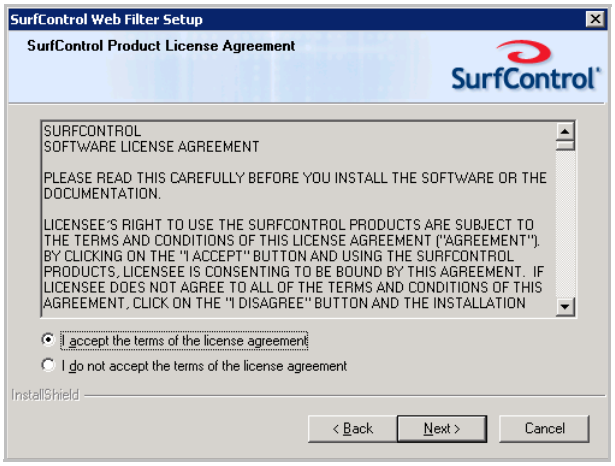
If you have an available Microsoft SQL Server, or you have installed SQL Server Express, you can install Web Filter V5.5:

1 Download Web Filter V5.5 from the SurfControl website then navigate to this file and double-click **setup.exe.** This will start the installation process.

2 The first screen you will see is the **Welcome** screen:

Click **Next**.

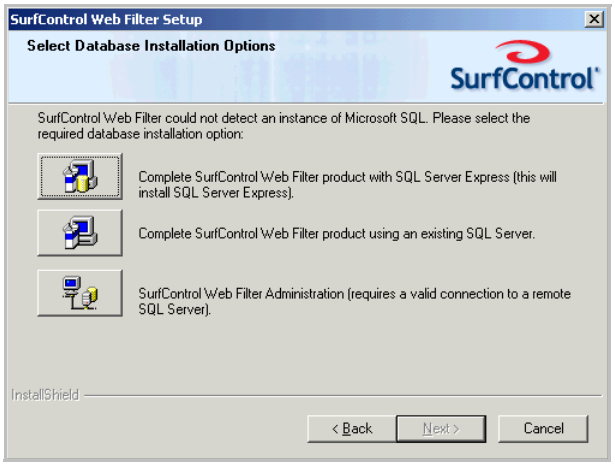
3 The **License Agreement** screen is displayed:



Select **I accept the terms of the license agreement**.

4 Click **Next.**

5 If the setup program does not detect a suitable database, the **Select Database Installation Options** is displayed. .



Note: If you have already installed SQL Server Express or SQL Server, this screen will not display.

6 You can now choose one of the following database options:

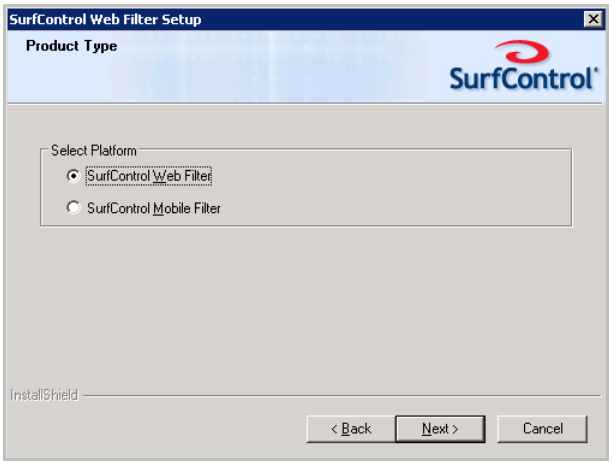

– Install the complete product which will also install SQL Server Express.


– Install the complete product using an existing SQL Server database.


– Install the Remote Administration version of Web Filter.

7 Click **Next**.

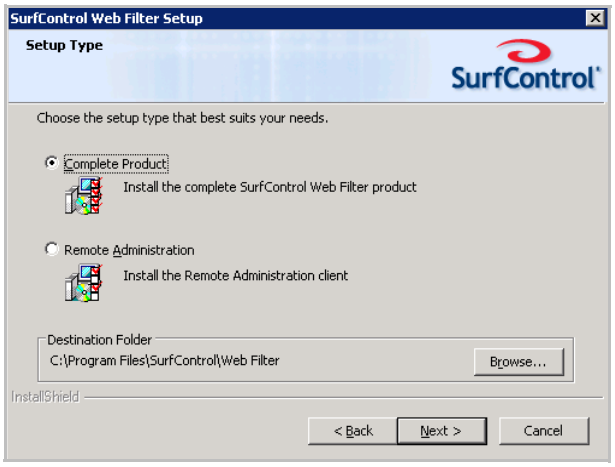
8 The **Product Type** screen is displayed.



Select **SurfControl Web Filter**.

9 Click **Next**.

10 The **Setup Type** screen is displayed.



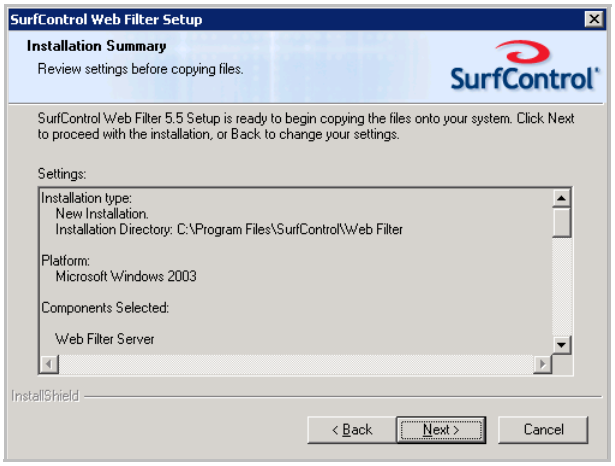
This screen enables you to specify how you want Web Filter to be installed:

- **Complete Product** - Select this option to install the complete SurfControl Web Filter program.
- **Remote Administration** - This enables you to access and manage the Web Filter server from any machine on your network.

  The setup program installs Web Filter to a default path of `c:\program files\SurfControl\Web Filter`. If you want to install Web Filter to a different location on the server, click **Browse** and navigate to the location.

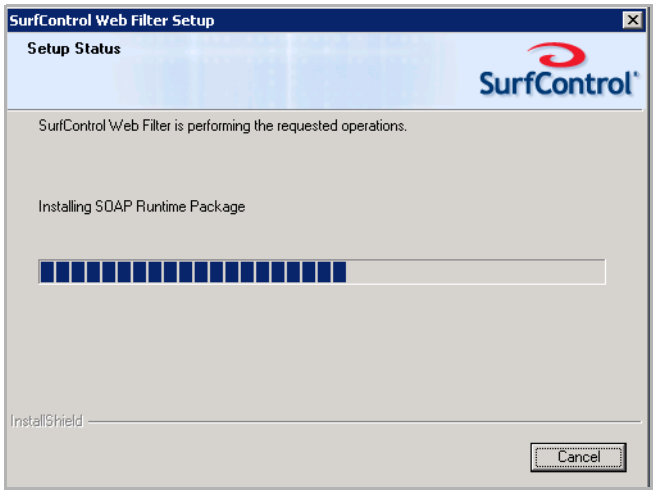
11 Once you have selected your setup type, click **Next**.

12 You will now see a screen giving you a summary of the installation options you have chosen:



Review your settings before starting the installation. When you are ready, click **Next**.

13 A status bar will indicate that the Web Filters are being copied to the server:



14 Once the files are copied across an Install Wizard Complete screen will indicate that Web Filter has been successfully installed:

Click **Finish** to close the setup program. The **Configuration Wizard** will launch automatically. The Configuration Wizard will start immediately. See "Configuring Web Filter" on page 36.

You can exit the Configuration Wizard and run it later, but you must complete the steps in the Wizard before Web Filter can start filtering Web content.

Note: If you are asked to restart your computer the Configuration Wizard will begin automatically after the computer has restarted.

CHANGES TO THE SERVER

The Web Filter setup program makes the following changes to the server:

- Places the WebFilter icon  in the Notification Area at startup.

  From this icon, you can perform the following actions:

  – Stop or start the Web Filter and Scheduler services.
  – Configure the Web Filter service settings.
  – Serialize the product from the About dialog box.

  If the Web Filter Service has been stopped, the WebFilter icon  becomes grayed out.

Note: On a Web Filter Remote Administration client, the grayed out icon is placed in the Notification Area to indicate that the service is not running locally.

- Creates additional necessary registry entries.
- Creation of the SurfControl_WebFilter database (default name `SurfControl_WebFilter`).
- Addition of the following services:
  – Web Filter service
  – Scheduler service
  – Remote Administration service
  – Audit Logger service
  – Virtual Control Agent service (license-holders only)
  – Corporate Network Detection Service (CNDS)

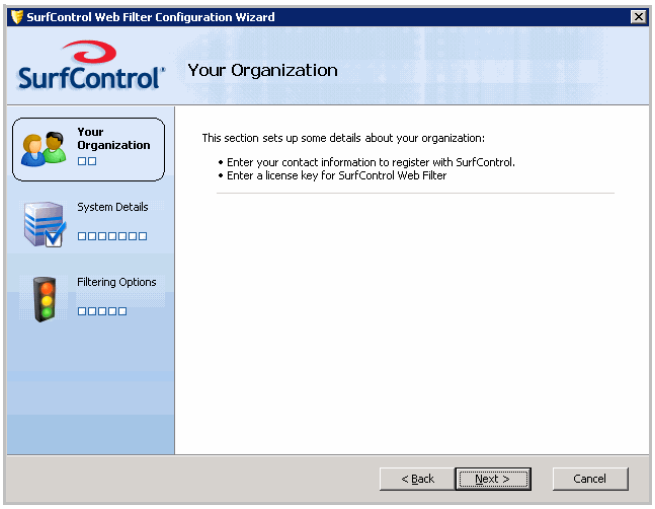
CONFIGURING WEB FILTER

The wizard will launch after you have finished the complete installation process on your Web Filter server. Perform the following steps.

1 As soon as the setup program is complete, the **Configuration Wizard** will start:

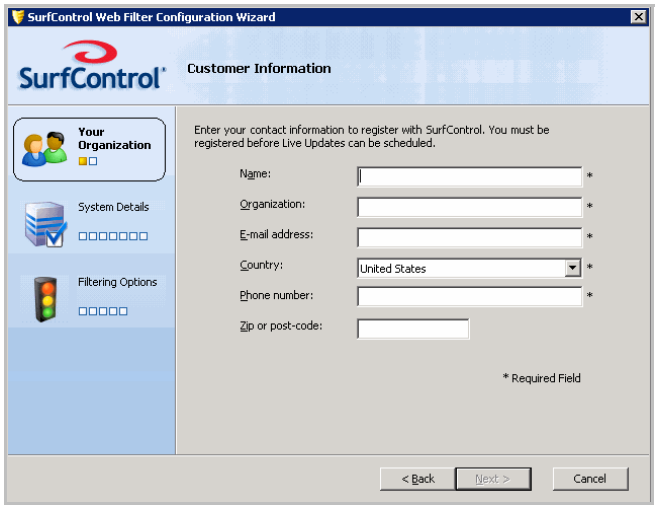
Click **Next**.

2 The **Your Organization** screen is displayed. This screen outlines the information you will enter in this section:



Click **Next**.

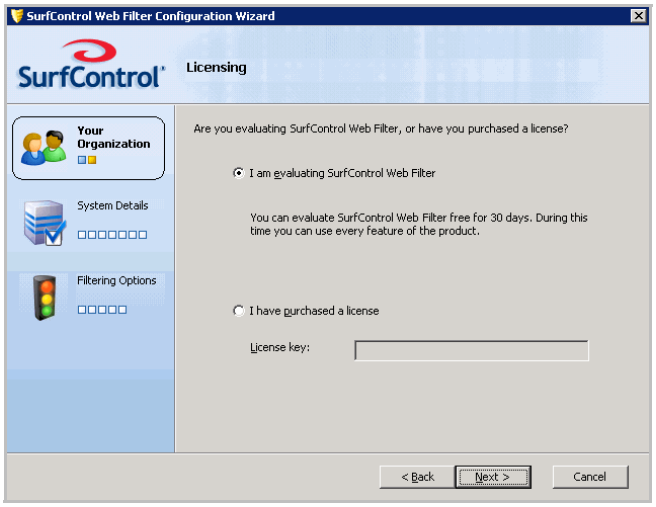
3 The **Customer Information** screen is displayed:



Fill in your details to register with SurfControl. Registered users can schedule live updates of the Internet Threat Database.

4 Click **Next**.

5 The **Licensing screen** is displayed:

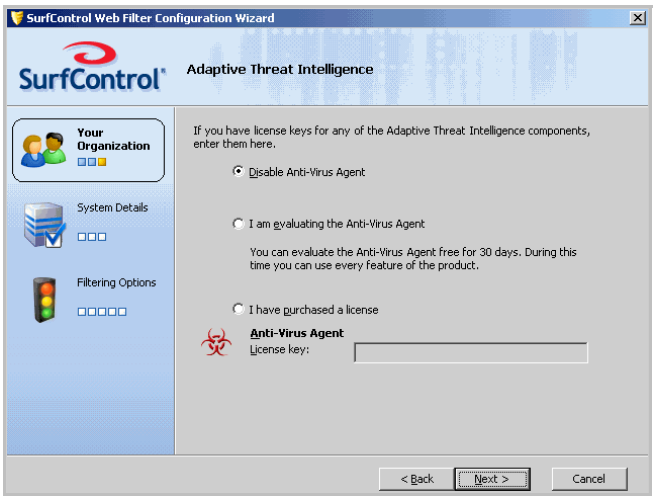


- If you are an evaluating customer, select **I am evaluating SurfControl Web Filter**.
- If you have purchased a Web Filter license, select **I have purchased a license** and enter your license key.

Note: If you have purchased Web Filter but do not have a license key, contact SurfControl Sales.

6 Click **Next**.

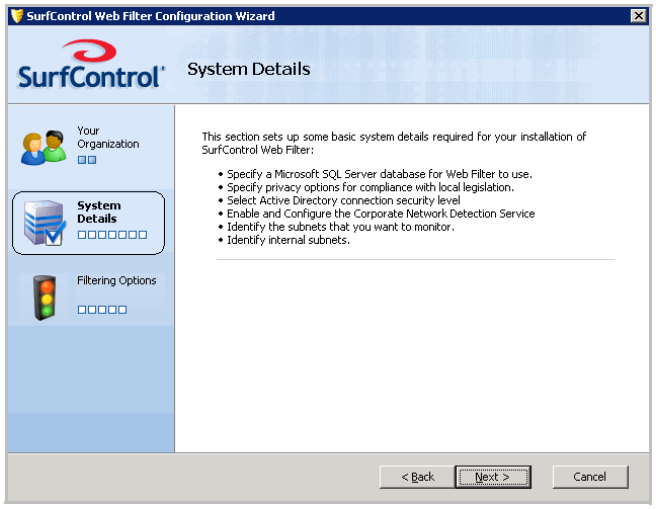
7 If you have entered a Web Filter license key, the **Adaptive Threat Intelligence** screen is displayed:



- Select **Disable Anti-Virus Agent** if you don't want to use the Anti-Virus Agent. You can enable it following installation by selecting **Prevent infectious content** from the Content tab in the Web Filter Settings. See Chapter 9 of the Administrator's Guide for more details.
- Select **I am evaluating the Anti-Virus Agent** if you haven't purchased a license for it. The evaluation lasts for 30 days.
- If you have purchased a license, select **I have purchased a license** and enter the license key.
- If you have purchased the Anti-Virus Agent but do not have a license key, contact SurfControl sales.

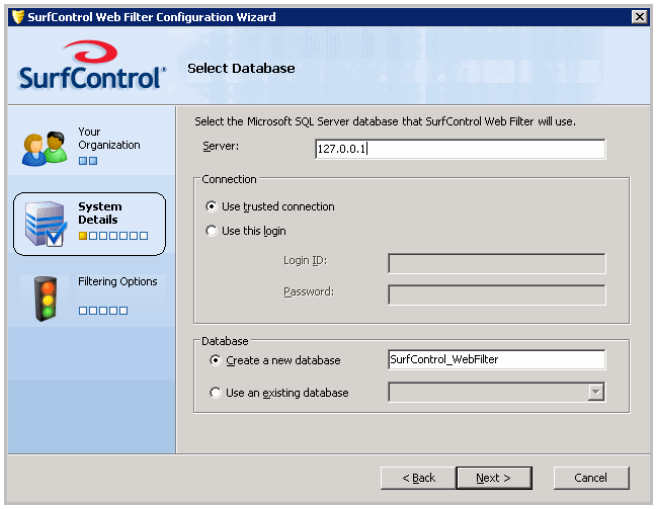
8 Click **Next**.

9 The **System Details** screen is displayed:



This screen outlines the information you will enter in this section. Click **Next**.

10 The **Select Database** screen is displayed:

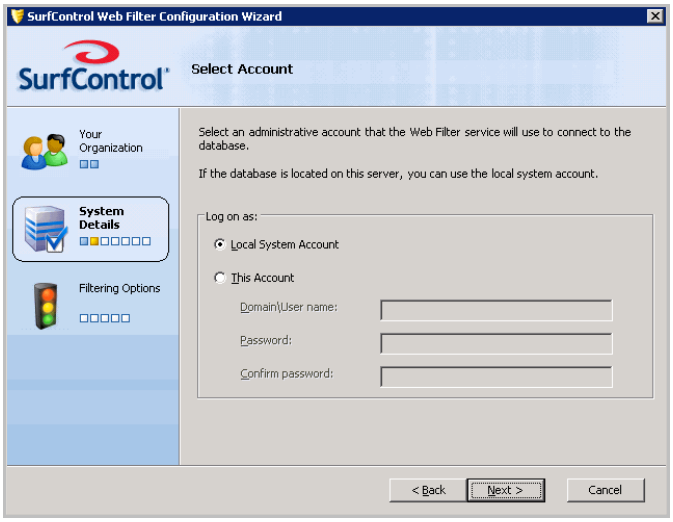


Fill in the fields as follows:

- **Server** - Enter the name or IP address of the server where your SQL Server Express, or SQL Server database is located.
- **Connection -** Specify how you want Web Filter to connect to the database. Web filter can either log in using your database's SA username and password, or using a trusted connection.
- **Database -** Specify whether you want to use an existing Web Filter database, or create a new one.

11 Click **Next**.

12 The **Select Account** screen is displayed:

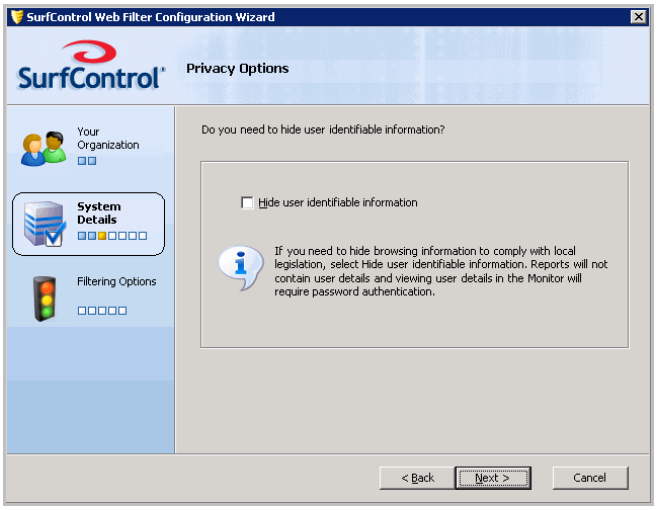


Choose how Web Filter will log on to your database.

- If your database is located on the same server as Web Filter, select Use Local System Account.
- If your database is hosted remotely, on another server, select This Account then enter the Domain and User name, with the corresponding Password for that user.

13 Click **Next**.

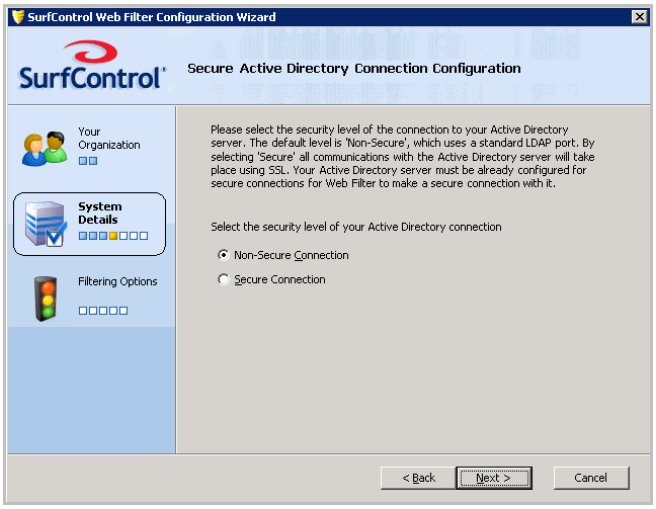
14 The **Privacy Options** screen is displayed. (This screen will not appear if you selected an existing database in Step 7):



If you need to hide user information to comply with regional legislation, select **Hide user identifiable information**.

15 Click **Next**.

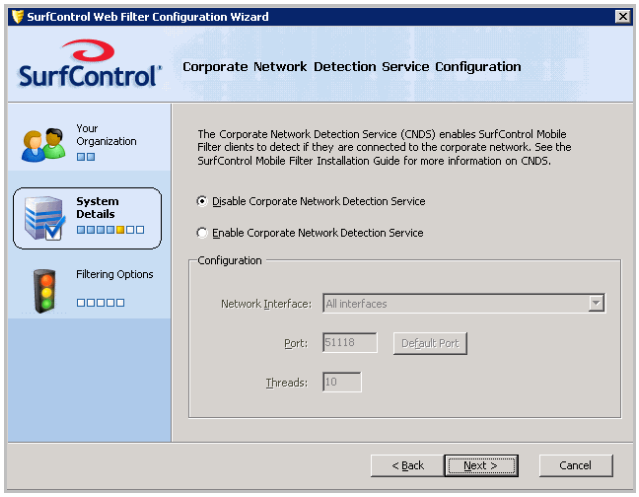
16 The **Secure Active Directory Connection Configuration** screen is displayed:



By default a non-secure connection is made to your Active Directory server. To change this to a secure SSL connection, select **Secure Connection**.

17 Click **Next**. Web Filter will attempt to make a secure connection.

18 You will now see the **Corporate Network Detection Service Configuration** screen:



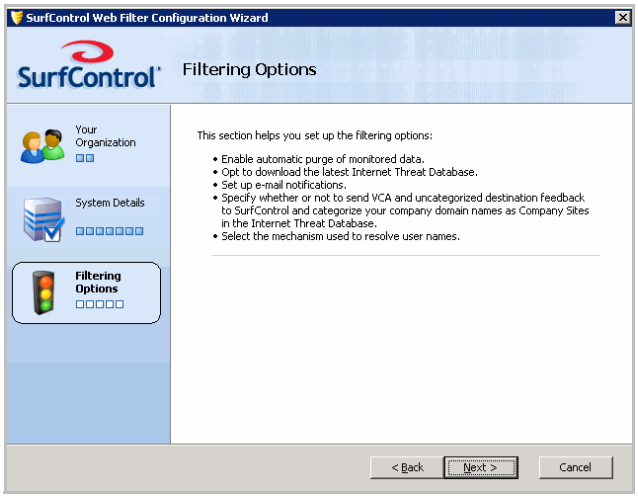
This service is used by SurfControl Mobile Filter to detect when clients are connected to a corporate Web Filter server, which then takes over the filtering of the device from the Mobile Filter client. This service must be installed on the Web Filter server.

- If you don't plan to install Mobile Filter, select **Disable Corporate Network Detection Service** (the default option).
- If you are installing Mobile Filter, select **Enable Corporate Network Detection Service**. For more information on this service, consult the SurfControl Mobile Filter Installation Guide.

Caution: SurfControl recommends leaving the configuration options at the default setting, unless advised to change them by Technical Support. You can change them later by selecting Configure Corporate Network Detection Service from the SurfControl Web Filter Start menu.

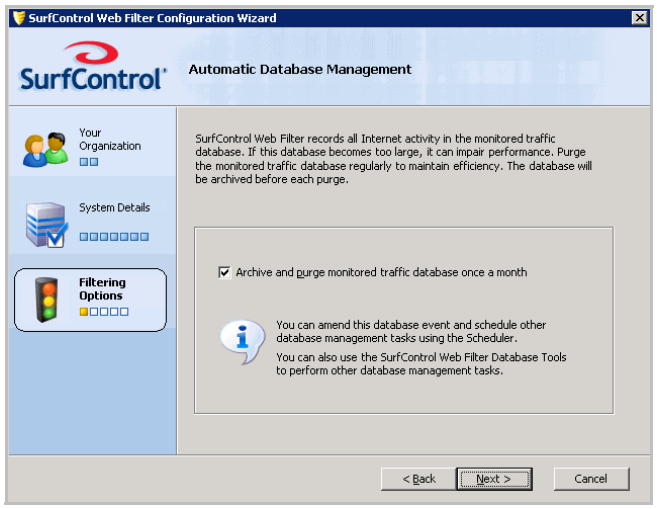
19 Click **Next**.

20 The **Filtering Options** screen outlines the information you will enter in this section:



Click **Next**.

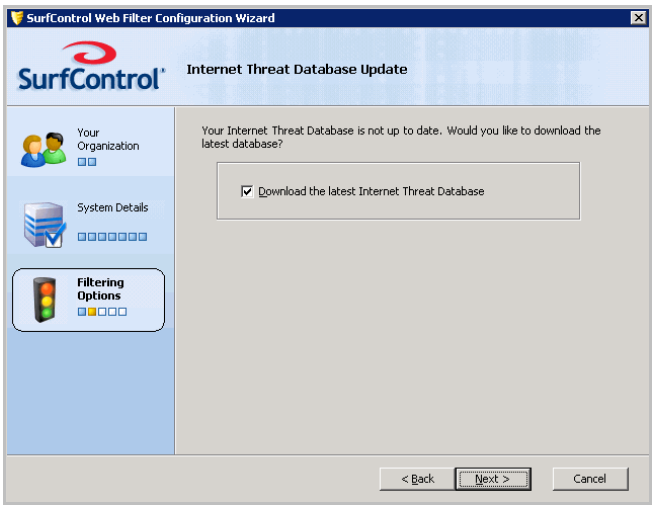
21 The **Automatic Database Management** screen is displayed:



To keep your database working efficiently, select **Archive and purge monitored traffic database once a month**.

22 Click Next.

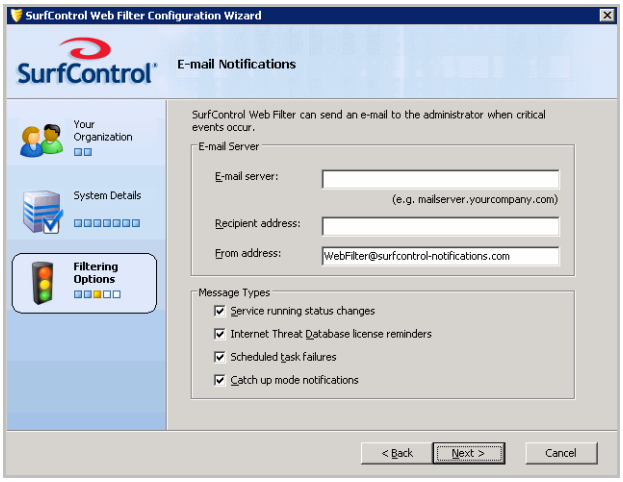
23 The **Internet Threat Database Update** screen is displayed:



For maximum protection you need the latest threat information. Select **Download the latest Internet Threat Database.**

24 Click **Next**.

25 The **E-mail Notifications** screen is displayed:



Web Filter can notify you when system events occur. Fill in the fields as follows:

- **E-mail Server:** Enter the name or IP address of the e-mail server for your domain. Web Filter will use this e-mail server to send notifications.
- **Recipient address:** Enter the e-mail address of the systems administrator.
- **From address**: enter the address that the notification e-mails will be delivered from.

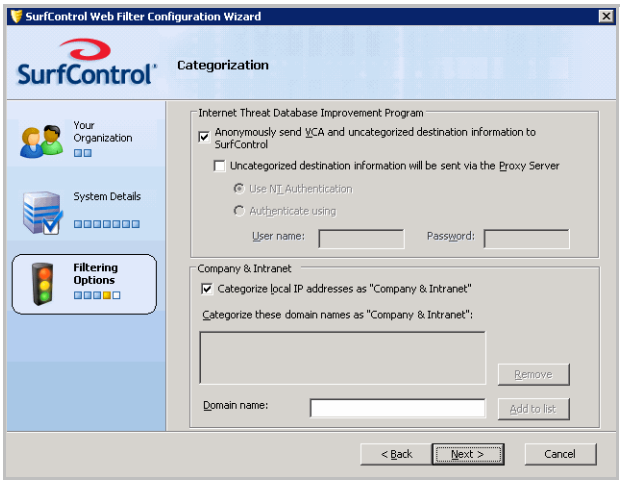
Caution: Entering E-mail server, Recipient and From e-mail address details on this screen will overwrite any settings present in ISA Server for the 'Service not responding' and 'Intrusion detected' alerts.

Specify which **Message Types** you want to be notified of. Choose any or all of the following:

- **Service running status changes** - Select this option if you would like to be notified about changes in the Web Filter Service status.
- **Internet Threat Database license reminders** - Select this option if you want to be notified about the category database subscription expiration.
- **Scheduled task failures** - Select this option if you want to be alerted about any scheduled tasks which fail to run.
- **ISA 2004 event notifications** (not available for ISA Server 2000) - Select this option if you want to be alerted to Microsoft events which are specific to ISA 2004 or 2006.

26 When you have made your choices, click **Next**.

27 The **Categorization screen** is displayed:



28 Select the **Anonymously send VCA and uncategorized destination information to SurfControl** check box, if you want to send uncategorized web site information anonymously to SurfControl. This helps to improve the effectiveness of the Internet Threat Database for future updates.

29 Select the **Uncategorized destination information will be sent via the proxy server** check box if your computer accesses the Internet via a proxy server.

30 Select **Use NT Authentication** if you want the proxy server to validate the VCA by using NT authentication.

OR

31 If you want to use a different user name and password to access the proxy server, select **Authenticate using** and enter the logon credentials.

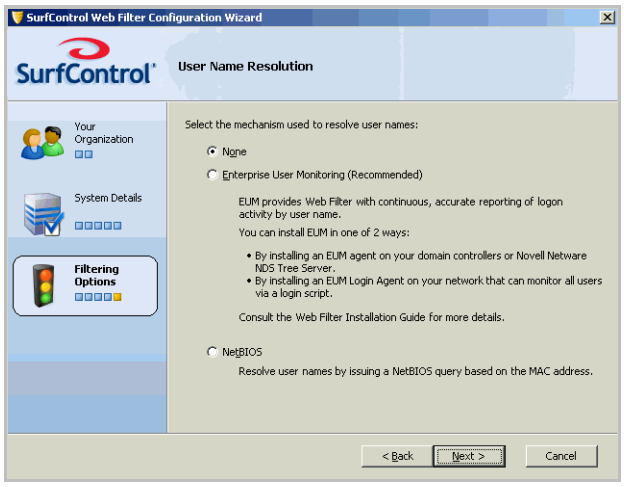
32 Select the **Categorize local IP addresses as 'Company & Intranet'** check box if you want to categorize your organization's domains as belonging to the Company and Intranets category. This means that, once you have added your domains, users visits to your organization's Web site or intranet will be logged under this category.

33 Enter the domain name into the Domain name text field (without entering the http://www prefix).

34 Click **Add to list**.

35 Click **Next**.

36 The **User Name Resolution** screen is displayed:



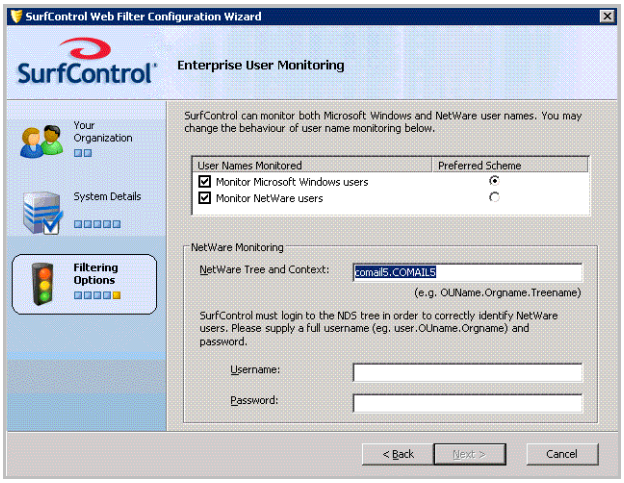
By default, User Name Resolution is not selected. Choose one of the following:

- **Enterprise User Monitoring** (recommended)
- **NetBIOS**

As an alternative, you can resolve user names via the ISA Server. See "ISA Server Authentication" on page 12 for further details. You can change the way you resolve user names following installation from the Web Filter Settings in the Web Filter Manager > Maintenance options.

37 Click **Next**.

38 If you are installing on a Novell NetWare environment, and selected Enterprise User Monitoring in step 17, the **Enterprise User Management** screen is displayed:



You have the following options:

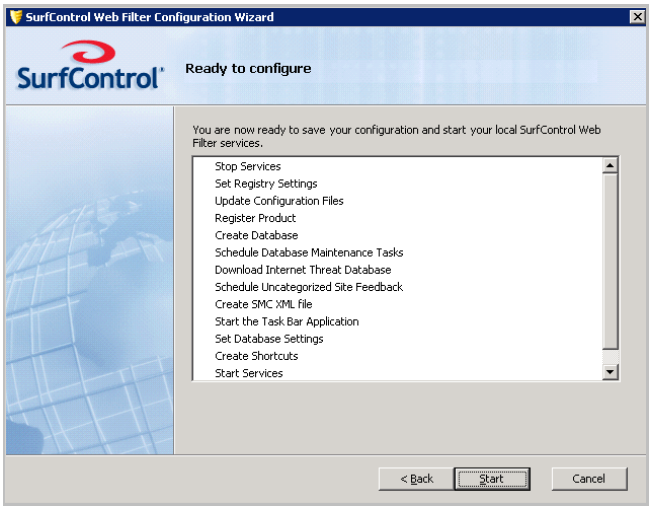
- **User Names Monitored** - You can monitor by either Windows or NetWare users, or both (the default). You can also select which is your preferred scheme.
- **NetWare Monitoring** - Your NetWare Tree and Context details are automatically displayed in this field.

- **Username and Password** - You need to enter a valid NDS tree username and password to enable Web Filter to identify NetWare users.

Note: You can select EUM during the installation process, and enter the details once the installation is complete. Information can be entered into the User Name Resolution tab in the Web Filter Settings. See Chapter 9 of the Administrator's Guide for more details.

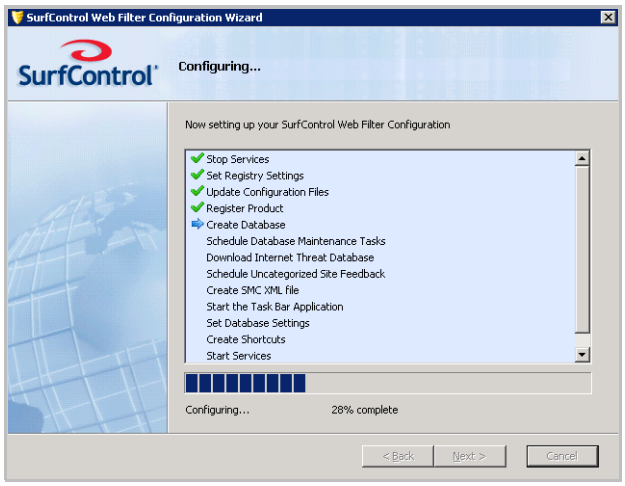
39 Click **Next**.

40 The **Ready to Configure** screen is displayed.



You can see a list of the tasks that the Configuration Wizard will perform to configure Web Filter. Click **Start**.

41 The **Configuring** screen is displayed.



A blue arrow shows the task currently in progress. As each task is completed, you will see a green check.

- If there is a problem with a task, you will see a warning icon ⚠ next to it. You can either go **Back** to change your settings, or **Skip** the task and move on to the next one.

- If there is a serious problem with a task, you will see a failure icon next to it. If this happens, the **Skip** button will be disabled and you must go back to correct your settings.

Note: If you skip a task, Web Filter may not filter traffic effectively.

42 The **Configuration Complete** screen is displayed.

You will need to install SurfControl Report Central to run reports on the internet traffic monitored by Web Filter. This is available from a product DVD or as a download from http://www.surfcontrol.com.

43 Click **Finish**.

Web Filter is now ready to start protecting your network from Internet Threats.

INSTALLING SERVICE PACK 3

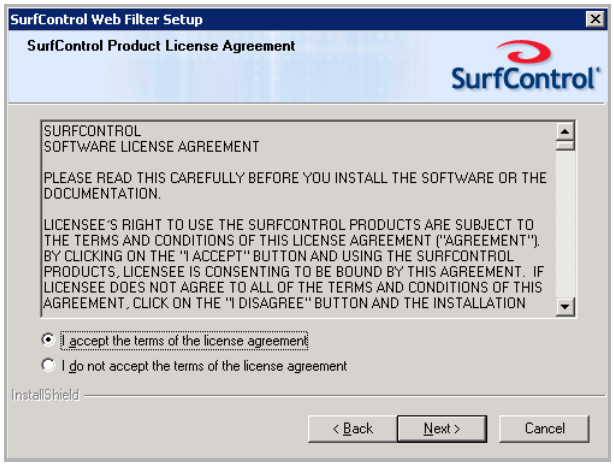
This section contains information on Installing Web Filter Service Pack 3. You can cancel the installation at any time by clicking **Cancel**. You will have to restart the installation process if you decide to install it again at a later date.

1 Download the service pack from the SurfControl web site to a suitable location.

2 Double-click **setup.exe** to start the installation process. You will now see the Welcome screen:

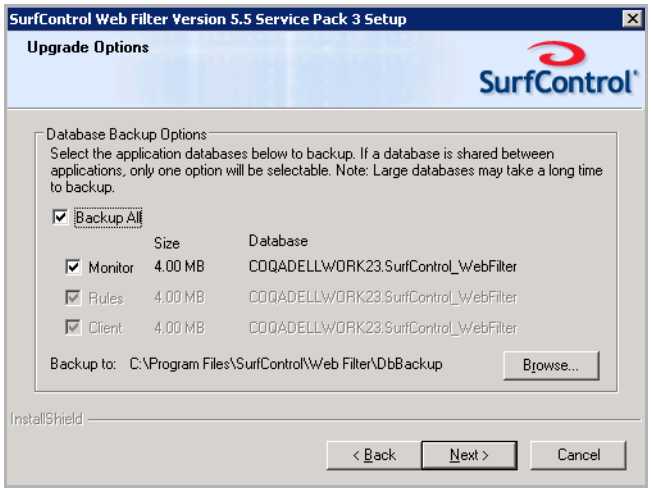
3 Click **Next**.

4 When you see the **License Agreement** screen, select **I accept the terms of the license agreement**:



5 Click **Next**.

6 You can now make a backup of your existing application databases using the Upgrade Options screen:



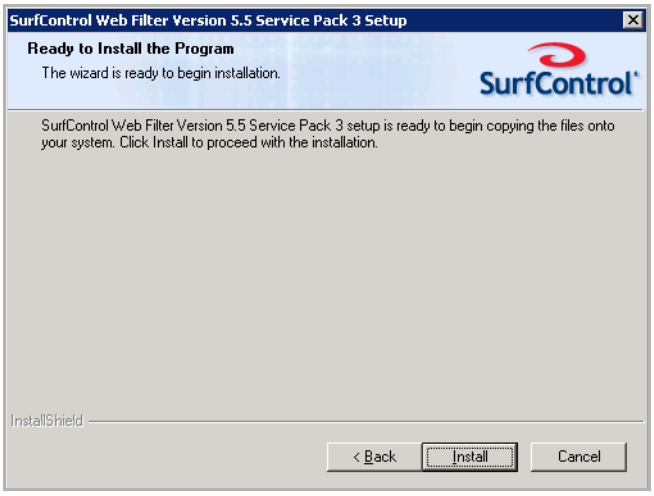
This will enable you to 'roll back' to your previous database, should this be necessary:

- Select **Backup All** to backup all of the available databases
  OR
- Select the database you want to back up from the list.

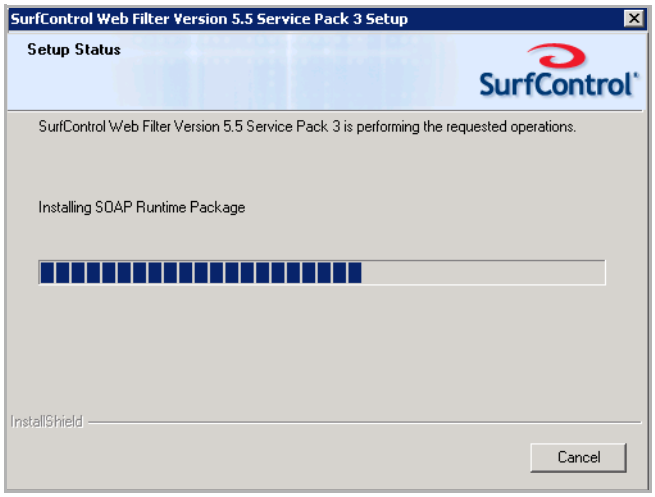
Note: If a database is shared with more than one application, you will only be able to select one of the applications that uses it.

7 Click **Next**.

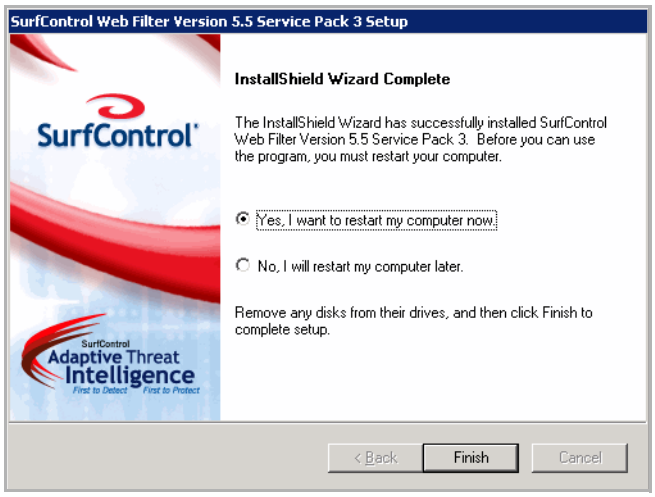
8 You will now see a screen informing you that the wizard is ready to install the service pack:



9 Click **Install** to start the installation. A progress bar will indicate how the installation is progressing:



10 You should now see the Install Wizard Complete screen:



Choose when to restart the computer: now or later.

11 Click **Finish** to finish the installation.

Chapter 4

Further Configuration

POST INSTALLATION TASKS

Following the installation of Web Filter, there are a number of tasks you may need to perform. Some apply to all installations, others are dependent on your network configuration or operating system set up.

ALL INSTALLATIONS

The following procedures need be performed after configuring Web Filter.

- Set up **User Name Resolution**. (page 53)
- Installation of **SurfControl Report Central**. (page 59)

FIREWALL POLICY RULES FOR ISA SERVER 2004 AND 2006

When Installing Web Filter on a Windows Server 2003 platform with ISA Server 2004 or 2006, the following procedures need to be performed for Web Filter to perform properly.

1 An ISA Server firewall policy rule must be set up that allows **Internet Threat Database updates**.

2 An ISA Server firewall policy rule must be set up that allows the **VCA** spider functionality to function properly.

3 An ISA Server firewall policy rule must be set up that allows the **Remote Administration client** to access the Web Filter Server.

4 An ISA Server firewall policy rule must be set up to allow remote access to **SurfControl Report Central**.

For more details on how to configure each policy rule, see "Firewall Policy Rules" on page 65.

NETWORK DEPENDENT

Depending on how your network and Web Filter server are set up, it may be necessary to follow the procedure for "Installing the Remote Administration Client" on page 60. This enables you to access the Web Filter server from any machine on your network.

USER NAME RESOLUTION

By default, SurfControl Web Filter resolves user names by issuing a NetBIOS query based on the MAC address. Web Filter also includes the **Enterprise User Monitor (EUM)** utility for resolving user names in a routed network. You can also use ISA Server to authenticate your users. See "ISA Server Authentication" on page 12 for more details.

For more details on how EUM works, see "ISA Server Authentication" on page 12.

You can install EUM in one of the following ways:

- Install the **EUM Agent** on all your domain controllers.
- Install the **EUM Login Agent** on your network.
- Install **NetWareEUM** on your NDS Tree Servers.

INSTALLING THE EUM AGENT ON YOUR DOMAIN CONTROLLERS

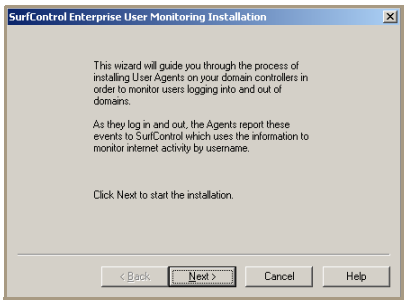
Before proceeding with the EUM Agent installation, check the following:

- Make sure that the Web Filter server has a static IP address.
- Make sure you have administrative privileges on all domain controllers where the User Agent will be installed.
- Make sure the Web Filter server is located in the correct domain.
- Make sure the firewall or router allows traffic through the provisioned port (default is 61695).
- For Windows NT domain controllers, make sure the security logs of the domain controllers are set to **overwrite events as needed**.
- Try to perform this procedure when there are few or no users on the network, or when a forced log off can be scheduled. This ensures the fastest, most accurate detection of users.

To install the EUM Agent on to your Domain Controllers:

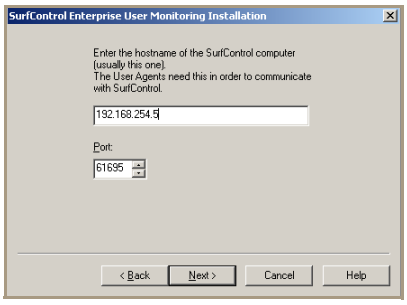
1 From the **Start** menu, select **Programs** > **SurfControl Web Filter** > **Enterprise User Monitoring** > **Install Enterprise User Monitoring**.

2 The **SurfControl Enterprise User Monitoring Installation** screen is displayed.



Click **Next**.

3 The **Hostname** screen is displayed.



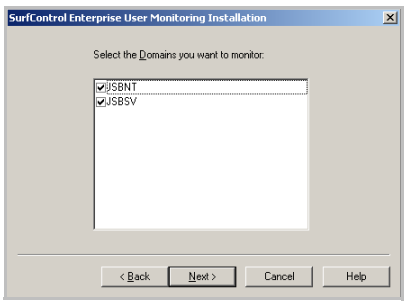
- Enter the IP address of the Web Filter server.

Note: SurfControl recommends entering the IP address instead of the hostname.

- Enter the port the User Agent and the Web Filter service should use to communicate (the default is 61695).

4 Click **Next**.

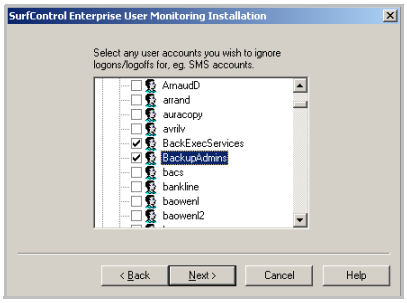
5 The **Domain List** screen is displayed.



Select the domains you want to receive user data from.

6 Click **Next**.

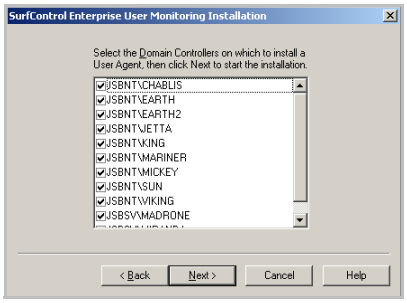
7 The **Ignore User Accounts** screen is displayed.



Select the user accounts whose logon or logoff activity does not need to be reported, for instance, Systems Management Server (SMS) and antivirus accounts.

8 Click **Next**.

9 The **Select Domain Controllers** screen is displayed.



Select the domain controllers whose user's logon and logoff activity Web Filter needs to monitor (this identifies the domain controllers where the User Agent will be installed).

10 Click **Next**. You have successfully installed Enterprise User Monitoring.

Note: Installation of the EUM UA on to Microsoft Windows 2000 domain controllers will require a restart. SurfControl recommends performing a manual restart of the domain controller.

Note: Failure to install EUM on all domain controllers can compromise the accuracy of user name resolution. If a domain controller is authenticating users, but not passing that data to Web Filter, user activity may be recorded under another user name.

Making changes to the EUM Agent configuration

After installing the EUM Agent, you may want to add further domain controllers to your EUM Agent configuration, specify more users that the EUM Agent should ignore, or specify how long your domain controllers should wait before sending configuration information to the Web Filter server(s).

The EUM Agent on the domain controller will wait ten minutes before checking for any changes made in the scua.ini file. The frequency of this can be changed by altering a registry setting on individual domain controllers. To change this value, perform the following:

1 On the domain controller, launch the Windows registry.

2 Depending on your operating system, navigate to one of the following keys:

- **Windows 2000 and 2003**

  HKLM\SOFTWARE\JSB\SurfControl SubAuth\ConfigReRead

- **Windows NT**

  HKLM\SOFTWARE\JSB\SurfControl EUM\ConfigReReadd

3 Edit the **ConfigReRead** value to the desired amount in seconds. By default, this value is set to 600 seconds (10 minutes).

There are two ways to add domain controllers or ignored users to the EUM Agent configuration:

- Use the EUM Installation Wizard.
- Manually edit the **scua.ini** file on each domain controller.

Using the EUM installation wizard. To start the wizard, follow the instructions in the Installing the EUM Agent on your domain controllers section. The installation wizard will automatically detect if the EUM Agent is already installed, and you can select additional domain controllers and/or ignored users to add to your existing EUM configuration.

Manually edit the scua.ini file. By default, the scua.ini file contains the host name and listening port number of the Web Filter server from which you initially installed the EUM Agent, and any ignored users you specified during the installation. You can add extra Web Filter servers to the file, if you want user login information to be returned from your domain controllers to multiple Web Filter servers. Below is an example of the scua.ini file:

```
[surfCONTROL_Services]

192.168.4.125=61695

192.168.4.119=61695

192.168.4.215=61695

[ignored_users]

domain\user1.test=1

domain\user2.test=1

domain\user3.test=1
```

To manually edit the file:

1 On the domain controller, open the **c:\Surfcontrol User Agent\scua.ini** file.

- To add a new Web Filter server, type an entry underneath the `[surfCONTROL_Services]` section, in either one of the following formats:

  `hostname=61695`

  `ip_address=61695`

- To manually add an ignored user, type an entry underneath the `[ignored_users]` section, in the following format:

  `domain\user.name=1`

2 Save the **scua.ini** file.

INSTALLING THE EUM LOGIN AGENT ON YOUR NETWORK

The Login Agent program and configuration file can be found in the following location in a default install:

`C:\Program Files\SurfControl\Web Filter\EnterpriseUserMonitoring\LoginAgent`

1 Copy the Login Agent program (**ScEumLoginAgent.exe**) and configuration file (**EumLogin.ini**) to a folder on your network that is accessible to all users.

2 Edit the configuration file (**EumLogin.ini**). For details on the settings, see "How to configure the file" on page 19.

3 Create or edit an existing log on and log off script to call the **ScEumLoginAgent.exe** program. See "Configuring a logon and logoff script" on page 20.

Note: If installing on Windows Server 2003, you will need to configure the Windows Firewall to accept traffic sent from the Login Agent Program. Please consult our Knowledge Base article 1775 for more details.

INSTALLING NETWAREEUM

Ensure Novell Client 32 was installed on the Web Filter server prior to Web Filter installation before proceeding with the following steps.

1 From the Web Filter server, log on to the Novell server with administrative rights.

2 Go to the **SYS** volume and create a directory (for example, nweum).

Note: When creating the directory, use DOS 8.3 naming conventions.

3 Under this directory, copy the files **nweum.nlm** and **scua.ini** from the Web Filter server (in a default installation they are located in `C:\Program Files\SurfControl\Web Filter\Netware`) to the Novell server.

4 From the NetWare Server console, load the **NLM** by typing:

`Load sys:\nweum\nweum.nlm`

5 Press **enter**.

Note: The system will not allow you to load the NLM if a copy is already running.

Automatically loading the NetWare EUM

To automatically load the NetWare EUM every time the server is restarted, perform the following steps:

1 Edit the `sys:\system\autoexec.ncf` file.

You can edit this file using any text editor from the workstation or from the NetWare Server by typing:

```
Load edit sys:\system\autoexec.ncf
```

2 Add the following line at the end of the file:

```
load sys:\nweum\nweum.nlm
```

3 Save the file.

Unloading the NetWare EUM

From the NetWare Server console, type the following: `unload nweum.nlm`

Add Web Filter Servers to NetWare EUM

Unload the NetWare EUM as described above.

1 Add the following details to the surfcontrol_services section of the **scua.ini** file

```
machine_name_or_IP_Address=Port number
```

The default port number is 61696. Port 61695 is used by Win 2000 and 2003 EUM architecture.

2 Save the **scua.ini** file.

3 Reload the NetWare EUM as described in Automatically loading the NetWare EUM.

Ignored users in NetWare EUM

1 Unload the NetWare EUM as described in Unloading the NetWare EUM.

2 Edit the `[Ignored Users]` section of the **scua.ini** file. The format for adding ignored users is as follows:

```
unique_user_key=fully_qualified_username_in_the_NDS_tree
```

For example:

```
user1=admin.NW_5_1_SURF
user2=tester.accounting.NW_5_1_SURF
```

3 Save the **scua.ini** file.

4 Reload the NetWare EUM as described in Automatically loading the NetWare EUM.

INSTALL SURFCONTROL REPORT CENTRAL

To produce reports on the Internet traffic monitored by Web Filter, you need to install SurfControl Report Central, either as a download from http://www.surfcontrol.com, or from a product DVD.

INSTALLING THE REMOTE ADMINISTRATION CLIENT

From the Remote Administration Client installation you can:

- View monitored traffic.
- Create and edit rules.
- Run reports.
- Start and stop the Web Filter Service.
- Start and stop the Scheduler Service.
- Access the Real-Time Monitor.

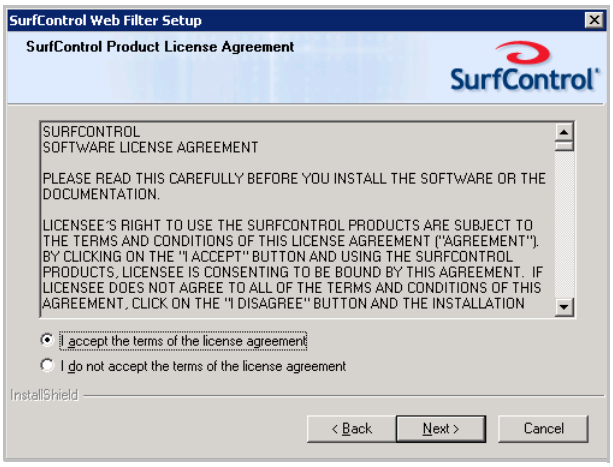
Perform the following set of instructions to install the **Remote Administration Client**:

1 Locate the downloaded SurfControl Web Filter file (**setup.exe**).

2 Double-click **setup.exe** to start the installation process. The InstallShield Wizard loads, followed by the SurfControl **Web Filter Setup** screen.

Click **Next**.

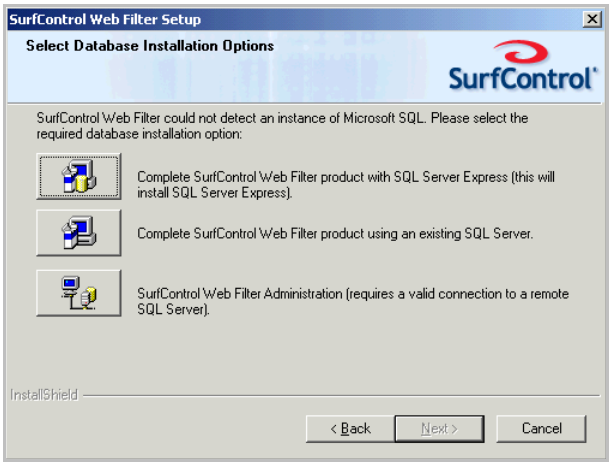
3 The **License Agreement** screen is displayed.



Select **I accept the terms of the license agreement**.

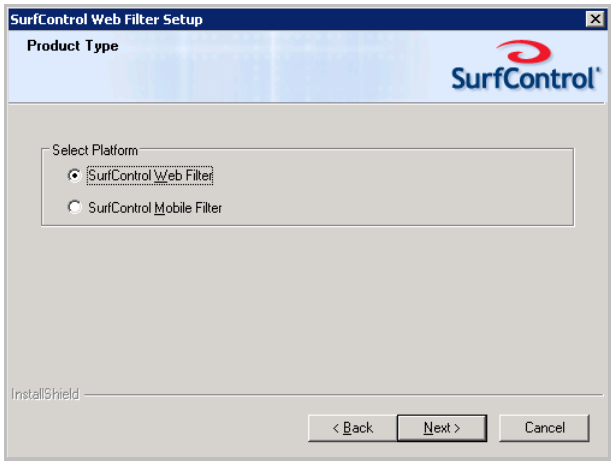
4 Click **Next**.

5 The **Select Database Installation Options** screen is displayed.



Select **SurfControl Web Filter Administration**.

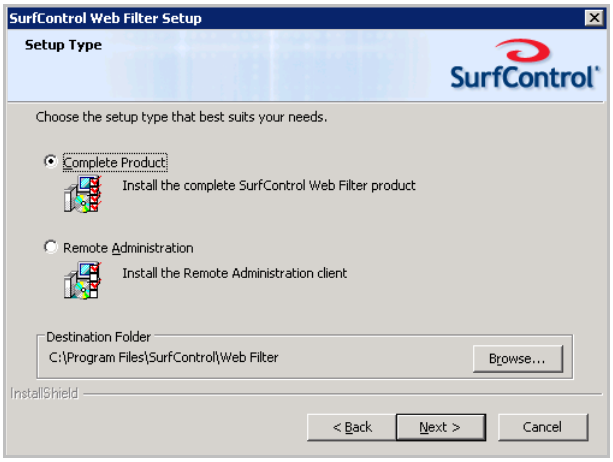
6 The **Product Type** screen is displayed.



Select **SurfControl Web Filter**.

7 Click **Next**.

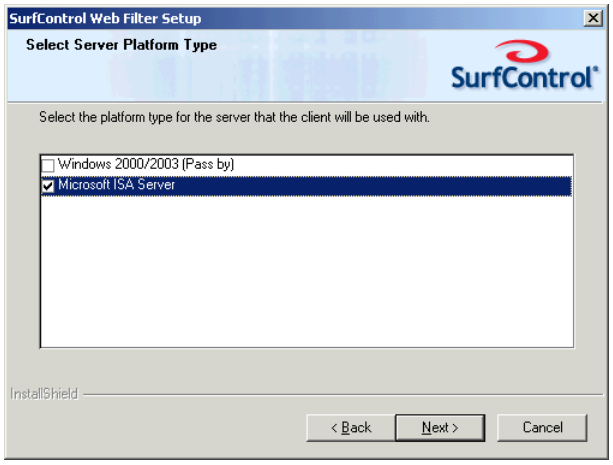
8 The **Setup Type** screen is displayed.



Select **Remote Administration**.

9 Click **Next**.

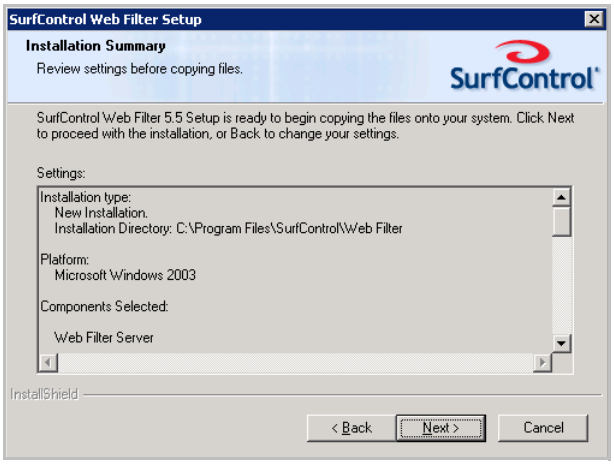
10 The **Select Server Platform Type** screen is displayed.



Select **Microsoft ISA Server**.

11 Click **Next**.

12 The **Installation Summary** screen is displayed.



Review your settings before starting the installation and click **Next**.

13 The **InstallShield Wizard Complete** screen is displayed.

14 Click **Finish**.

The **Configuration Wizard** will start automatically.

Note: The Configuration Wizard for the Remote Administration is a subset of the Complete Product version.

The Remote Administration Client and Windows Vista

Windows Vista provides user security in the form of User Account Control (UAC). UAC enables System Administrators to run most applications with limited privileges, but gives the option to elevate certain programs which need Administrator authentication to run. Standard users follow the same process, but they will have to supply an Admin password to perform program elevation.

If your Remote Administration client is installed on Windows Vista, and UAC is enabled, each remote Web Filter application will need the permission of an elevated user to start. This means that you will either have to be logged in as Administrator, or as a standard user who knows the Admin password.

FIREWALL POLICY RULES

When installing Web Filter on ISA Server 2004 or 2006 and Windows Server 2003, the following firewall policy rules should be set up to enable Web Filter to function correctly:

- A firewall policy rule must be set up that allows **Internet Threat Database updates**.
- A firewall policy rule must be set up that allows the **VCA spider functionality** to function properly.
- A firewall policy rule must be set up that allows the **Remote Administration client to access the Web Filter Server**.
- A firewall policy rule must be set up that allows remote access to **SurfControl Report Central** (to be created after installing Report Central).

The following procedures detail how to set up firewall policy rules on Microsoft ISA Server 2004.

ALLOW INTERNET THREAT DATABASE UPDATES

1 Select **Firewall Policy** from **ISA Server Management**.

2 From the System Policy Tasks select **Show System Policy Rules**.

3 Right-click **Allow HTTP/HTTPS requests from ISA Server to specified sites** and select Properties.

4 From the **To** tab, select **System Policy Allowed Sites** and click **Edit**.

5 Click **Add**.

6 Enter ***.surfcontrol.com**.

7 Click **Apply**, then **OK** to close the dialog box.

8 Click **Apply** in the Firewall Policy window.

ALLOW VCA SPIDER FUNCTIONALITY

This procedure is in 2 parts. You must firstly configure the Web Filter server browser (Internet Explorer) and the VCA. You then need to create a firewall policy rule in ISA Server.

Configure IE and the VCA

1 Check that Internet Explorer on the ISA Server is able to access the internet.

2 From the Web Filter Manager, select **Custom Categorization** from Content Protection.

3 Select the **VCA Settings** tab.

4 Select the **Impersonate Internet Explorer** check box.

5 Select the **Use Proxy** check box.

6 If your proxy allows for integrated authentication, select **Use NT Authentication**, otherwise you must enter a User Name and Password for VCA to access the proxy.

7 Click **Apply**, then **OK** to close the dialog box.

8 Open Internet Explorer.

9 Select **Internet Options** from the **Tools** menu.

10 From the **Connections** tab, click **LAN Settings**.

11 Select **Use a Proxy Server**.

12 Select **Bypass proxy server for local addresses**.

13 Click **OK**.

14 Click **OK** again to close the dialog box.

Configure a Firewall Policy Rule for the VCA

1 Select **Firewall Policy** from the **ISA Server Manager**.

2 Select **Create New Access Rule** from the **Tasks** tab.

3 From the Wizard, give your new rule a name. Click **Next**.

4 Select **Allow**. Click **Next**.

5 Select **All Outbound Traffic**. Click **Next**.

6 From **Access Rule Sources**, click **Add**.

7 Expand the Networks folder and select **Local Host**. Click **Add**, then **Close**.

8 Click **Next**.

9 From **Access Rule Destinations**, click **Add**.

10 Expand the Networks folder and select **External**. Click **Add**, then **Close**.

11 Click **Next**.

12 Select **All Users** (the default) or select the users you wish to have access. Click **Next**.

13 Click **Finish**.

14 Click **Apply** in the Firewall Policy window.

ALLOW THE REMOTE ADMINISTRATION CLIENT ACCESS

Firstly install the Remote Administration Client (see "Installing the Remote Administration Client" on page 60). Ensure that NetBIOS and RPC are enabled on both the remote computer and the server. Then create the firewall policy rule as set out in the instructions below.

1 Select **Firewall Policy** from the **ISA Server Manager**.

2 Select **Create New Access Rule** from the **Tasks** tab.

3 From the Wizard, give your new rule a name. Click **Next**.

4 Select **Allow**. Click **Next**.

5 Select **Selected Protocols** from the drop-down list box. Click **Add**.

6 From the **Add Protocols** dialog box, select **Protocol** from the New menu. The **New Protocol Definition Wizard** will start.

7 Enter a name for your protocol. Click **Next**.

8 From the **Primary Connection Information** screen, click **New**.

9 Select **UDP** from the **Protocol type** drop-down list box.

10 Select **Send** from the **Direction** drop-down list box.

11 Enter **1024** in the **Port Range From** field.

12 Enter **65535** in the **Port Range To** field.

13 Click **OK**, then **Next**.

14 Select **No** from the **Secondary Connections** screen. Click **Next**.

15 Click **Finish**.

16 From the **Add Protocols** dialog box, expand the **User Defined** folder and select the Protocol you set up. Click **Add**, then **Close**.

17 From the **New Access Rule** Wizard, click **Next**.

18 From **Access Rule Sources**, click **Add**.

19 Expand the **Computer Sets** folder and select **Remote Management Computers**. Click **Add**.

20 Expand the **Networks** folder and select **Local Host**. Click **Add** then **Close**.

21 Click **Next**.

22 From **Access Rule Destinations**, click **Add**.

23 Expand the **Computer Sets** folder and select **Remote Management Computers**. Click **Add**.

24 Expand the **Networks** folder and select **External**. Click **Add**, then **Close**.

25 Click **Next**.

26 Select **All Users** (the default) or select the users you wish to have access. Click **Next**.

27 Click **Finish**.

28 Click **Apply** in the Firewall Policy window.

ALLOW REMOTE ACCESS TO SURFCONTROL REPORT CENTRAL (SRC)

1 Select **Firewall Policy** from the **ISA Server Manager**.

2 Select **Create New Access Rule** from the **Tasks** tab.

3 From the Wizard, give your new rule a name. Click **Next**.

4 Select **Allow**. Click **Next**.

5 Select **Selected Protocols** from the drop-down list box. Click **Add**.

6 From the **Add Protocols** dialog box, select **Protocol** from the **New** menu. The New Protocol Definition Wizard will start.

7 Enter a name for your protocol. Click **Next**.

8 From the **Primary Connection Information** screen, click **New**.

9 Select **TCP** from the **Protocol type** drop-down list box.

10 Select **Outbound** from the **Direction** drop-down list box.

11 Enter **8888** in the **Port Range From** field.

12 Enter **8888** in the **Port Range To** field.

13 Click **OK**, then **Next**.

14 Select **No** from the **Secondary Connections** screen. Click **Next**.

15 Click **Finish**.

16 From the **Add Protocols** dialog box, expand the User Defined folder and select the Protocol you set up. Click **Add**, then **Close**.

17 From the **New Access Rule Wizard**, click **Next**.

18 From **Access Rule Sources**, click **Add**.

19 Expand the **Computer Sets** folder and select **Remote Management Computers**. Click **Add**.

20 Expand the **Networks** folder and select **Local Host**. Click **Add** then **Close**.

21 Click **Next**.

22 From **Access Rule Destinations**, click **Add**.

23 Expand the **Computer Sets** folder and select **Remote Management Computers**. Click **Add**.

24 Expand the **Networks** folder and select **External**. Click **Add**, then **Close**.

25 Click **Next**.

26 Select **All Users** (the default) or select the users you wish to have access. Click **Next**.

27 Click **Finish**.

28 Click **Apply** in the **Firewall Policy** window.

Note: The firewall policy rule outlined above, sets remote access for the HTTP connection to SRC. If you want to use the HTTPS connection, you need to substitute port number 8888 with 8443.

Appendix

CONTACT TECHNICAL SUPPORT

Websense provides technical information about SurfControl products online 24 hours a day, including:

- latest release information
- searchable Knowledge Base
- show-me tutorials
- product documents
- tips
- in-depth technical papers

Access support on the Web site at:

www.websense.com/SupportPortal/

If you need additional help, please fill out the online support form at:

www.websense.com/SupportPortal/Contact.aspx

Note your case number. If you need to send Support files to help us diagnose your problem, do the following:

1. Select **Start > SurfControl Web Filter > Support Tools > Create Web Filter Support Files**. This creates an e-mail message containing a copy of your configuration files that will help Support to discover the reason for any problems you are having. These include:
   - Event Logs (System and Application)
   - A list of file Versions
   - Registry Keys
   - System Information
   - Trace Logs
2. Add your case number to the subject line of the email message.
3. Navigate to C:\Program Files\SurfControl\Web Filter\Support. In this directory you will find the following files:
   - Application.evt
   - System.evt
   - FileVersion.txt
   - registry.txt
   - systeminfo.txt
4. Zip or rar these files and attach them to the email.
5. Press Send.

If your issue is urgent, please call one of the offices listed below.

Location	Contact information
North America	+1 858-458-2940
France	Contact your Websense Reseller. If you cannot locate your Reseller: +33 1573 232 27
Germany	Contact your Websense Reseller. If you cannot locate your Reseller: +49 6951 709 347
UK	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 2030 244 401
Rest of Europe	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 2030 244 401
Middle East	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 2030 244 401
Africa	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 2030 244 401
Australia/NZ	Contact your Websense Reseller. If you cannot locate your Reseller: 1-800-881-011, Access Code 800-542-8609
Asia	Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884-4200
Latin America and Caribbean	Contact your Websense Reseller.

You will be routed to the first available technician, who will gladly assist you.

For the latest support information on SurfControl products, visit www.websense.com/SupportPortal/.

SALES AND FEEDBACK

For product and pricing information, or to place an order, contact Websense. To find your nearest Websense office, please visit our web site: www.websense.com